Acronis True Image™ 2017

Table of contents

1 Introduction 6

1.1 What is Acronis® True Image™? 6

1.2 New in this version 6

1.2.1 Alternatives to the removed features 7

1.3 System requirements and supported media 7

1.3.1 Minimum system requirements 7

1.3.2 Supported operating systems 8

1.3.3 Supported file systems 8

1.3.4 Supported Internet connection types 9

1.3.5 Supported storage media 9

1.4 Installing Acronis True Image 10

1.5 Activating Acronis True Image 11

1.6 Trial version information 12

1.7 Upgrading Acronis True Image 12

1.8 Technical Support 13

2 Getting started 15

2.1 User interface language 15

2.2 Protecting your system 15

2.2.1 Step 1. Backing up your computer 16

2.2.2 Step 2. Creating bootable rescue media 17

2.3 Backing up all data on your PC 18

2.4 Backing up your files 19

2.5 Cloning your hard drive 21

2.6 Recovering your computer 22

2.7 Recovering your files and folders 24

2.8 Acronis account 24

2.9 Getting started with Acronis Cloud 25

2.9.1 Subscription information 25

3 Basic concepts 27

3.1 Basic concepts 27

3.2 The difference between file backups and disk/partition images 28

3.3 Full, incremental and differential backups 29

3.4 FAQ about backup, recovery and cloning 31

3.5 Deciding where to store your backups 33

3.5.1 Preparing a new disk for backup 34

3.5.2 FTP connection 34

3.5.3 Authentication settings 35

3.6 Using Acronis Nonstop Backup 35

3.6.1 Acronis Nonstop Backup data storage 36

3.6.2 Nonstop Backup - Frequently asked questions 36

3.7 Backup file naming 37

Copyright © Acronis International GmbH, 2002-2016

3.8 Integration with Windows 38
3.9 Wizards 39
4 Backing up data 41
4.1 Backing up disks and partitions 41
4.2 Backing up files and folders 42
4.3 Backing up mobile devices 43
4.4 Backup options 44
4.4.1 Scheduling 46
4.4.2 Backup schemes 48
4.4.3 Notifications for backup operation 53
4.4.4 Excluding items from backup 54
4.4.5 Image creation mode 56
4.4.6 Backup protection 56
4.4.7 Pre/Post commands for backup 57
4.4.8 Backup splitting 57
4.4.9 Backup validation option 58
4.4.10 Backup reserve copy 58
4.4.11 Removable media settings 59
4.4.12 Error handling 59
4.4.13 File-level security settings for backup 60
4.4.14 Computer shutdown 61
4.4.15 Acronis Cloud cleanup 61
4.4.16 Online backup protection 61
4.4.17 Selecting a data center for backup 62
4.4.18 Performance of backup operation 62
4.5 Operations with backups 63
4.5.1 Backup operations menu 64
4.5.2 Sorting backups in the list 65
4.5.3 Validating backups 65
4.5.4 Backup to various places 66
4.5.5 Adding an existing backup to the list 66
4.5.6 Deleting backups and backup versions 66
4.5.7 Backing up to Acronis Cloud from several computers 68
4.5.8 Removing data from Acronis Cloud 68
5 Recovering data 69
5.1 Recovering disks and partitions 69
5.1.1 Recovering your system after a crash 69
5.1.2 Recovering partitions and disks 78
5.1.3 About recovery of dynamic/GPT disks and volumes 79
5.1.4 Arranging boot order in BIOS 81
5.2 Recovering files and folders 82
5.3 Searching backup content 83
5.4 Recovery from Acronis Cloud 84
5.4.1 Recovering data from online backups 84
5.4.2 Selecting a version to recover 85
5.4.3 Disk recovery from Cloud 86
5.5 Recovery options 89
5.5.1 Disk recovery mode 90
5.5.2 Pre/Post commands for recovery 90
5.5.3 Validation option 90

 Copyright © Acronis International GmbH, 2002-2016

5.5.4 Computer restart ... 91
5.5.5 File recovery options ... 91
5.5.6 Overwrite file options ... 91
5.5.7 Performance of recovery operation ... 92
5.5.8 Notifications for recovery operation ... 92
6 Archiving data ... 94
6.1 What is data archiving? ... 94
6.2 What is excluded from archives? ... 95
6.3 Cloud archiving vs. Online backup ... 95
6.4 Archiving your data ... 96
6.4.1 Data archiving options ... 96
6.5 Accessing your archived files ... 97
7 Protecting family data ... 98
7.1 What is family data protection? ... 98
7.2 Adding a new device to Online Dashboard ... 98
7.3 Backing up data remotely ... 99
7.4 Recovering data with Online Dashboard ... 100
7.5 Backing up a Facebook account ... 100
7.6 Recovering your Facebook account ... 101
8 Synchronizing data ... 102
8.1 About the Sync feature ... 102
8.2 How we ensure security of your data ... 102
8.3 What you can and cannot synchronize ... 102
8.4 Sync icons ... 103
8.5 Sync creation ... 104
8.5.1 Default sync ... 105
8.6 Versions of synchronized files ... 105
8.6.1 Reverting to a previous file version ... 105
8.7 How to clean up your space on Acronis Cloud ... 105
8.8 How to recover a deleted file ... 107
8.9 How to unlink a device from your account ... 107
9 Acronis True Image for mobile devices ... 109
9.1 Installing Acronis True Image for mobile devices ... 109
9.2 Backing up your mobile device to Acronis Cloud ... 110
9.3 Backing up your mobile device to a computer ... 110
9.4 Recovering mobile data with your mobile device ... 111
9.5 Recovering data to a new smartphone ... 111
9.6 Mobile app settings ... 112
9.7 Local destination of mobile backups ... 112
10 Disk cloning and migration ... 113
10.1 Disk cloning utility ... 113

 Copyright © Acronis International GmbH, 2002-2016

10.1.1 Clone Disk wizard ... 113
10.1.2 Manual partitioning ... 116
10.1.3 Excluding items from cloning ... 117
10.2 Migrating your system from an HDD to an SSD ... 118
10.2.1 What to do if Acronis True Image does not recognize your SSD ... 118
10.2.2 Migrating to SSD using the backup and recovery method ... 119
11 Tools ... 121
11.1 Creating bootable rescue media ... 122
11.1.1 Acronis Media Builder ... 122
11.1.2 Making sure that your rescue media can be used when needed ... 126
11.2 Acronis Startup Recovery Manager ... 131
11.3 Try&Decide ... 132
11.3.1 Using Try&Decide ... 135
11.3.2 Try&Decide options and notifications ... 136
11.3.3 Try&Decide: typical use cases ... 136
11.4 Acronis Secure Zone ... 137
11.4.1 Creating and managing Acronis Secure Zone ... 138
11.4.2 Acronis Secure Zone location ... 139
11.4.3 Size of Acronis Secure Zone ... 140
11.4.4 Acronis Secure Zone protection ... 140
11.4.5 Removing Acronis Secure Zone ... 141
11.5 Adding a new hard disk ... 141
11.5.1 Selecting a hard disk ... 142
11.5.2 Selecting initialization method ... 143
11.5.3 Creating new partitions ... 143
11.6 Security and Privacy Tools ... 145
11.6.1 Acronis DriveCleanser ... 145
11.6.2 System Clean-up ... 149
11.6.3 Hard Disk Wiping methods ... 155
11.7 Mounting an image ... 156
11.8 Unmounting an image ... 157
11.9 Acronis Universal Restore ... 157
11.9.1 Creating Acronis Universal Boot media ... 158
11.9.2 Using Acronis Universal Restore ... 160
12 Troubleshooting ... 162
12.1 Acronis System Report ... 162
12.2 Acronis Smart Error Reporting ... 163
12.3 Sending feedback to Acronis ... 164
12.4 How to collect crash dumps ... 165
12.5 Acronis Customer Experience Program ... 165
13 Glossary of Terms ... 167

Copyright © Acronis International GmbH, 2002-2016

1 Introduction

1.1 What is Acronis® True Image™?

Acronis True Image is an integrated software suite that ensures the security of all of the information on your PC. It can back up your documents, photos, email, and selected partitions, and even the entire disk drive, including operating system, applications, settings, and all of your data.

Backups allow you to recover your computer system should a disaster occur, such as losing data, accidentally deleting critical files or folders, or suffering a complete hard disk crash.

Online Backup allows you to store your files and disks on Acronis Cloud. Your data will be protected even if your computer is lost, stolen, or destroyed, and your data can be entirely recovered onto a new device, if needed.

Key features:

- Disk backup to a local storage and to Acronis Cloud (p. 41)
- File backup to a local storage and to Acronis Cloud (p. 42)
- Rescue bootable media (p. 122)
- Hard disk cloning (p. 113)
- Data archiving (p. 94)
- Family data protection (p. 98)
- File synchronization (p. 102)
- Security and privacy tools (p. 121)

Getting started

Learn how to protect your computer with two simple steps: "Protecting your system (p. 15)".

1.2 New in this version

- **Local archiving**—When you archive your old, large, or rarely used files, Acronis Cloud is not the only possible destination. You can also select local storage, including NAS, an external hard drive, or a USB flash drive. Your local archives are placed into Acronis Archive, which can be accessed in File Explorer under Favorites, along with your cloud archive.
- **Archive encryption**—To protect the archived data from unauthorized access, you can encrypt the archive with industry-standard AES (Advanced Encryption Standard) cryptographic algorithm with a 256-bit long key.
- **File search in backups**—When you recover your data, you can use search to easily find a specific file or folder in the selected backup. You can type the full file name or type a partial file name and use common wildcard characters (* and ?).
- **Auto-detection of NAS devices**—If you use NAS in your home network, Acronis True Image will detect it and suggest backing up to this device. All NAS devices are detected correctly even without Bonjour software installed on your computer.
- **Mobile device backup to local storage**—If you have an iOS or Android smartphone or tablet, you can protect your mobile data, such as photos, video files, contacts, and calendars. In addition to

Copyright © Acronis International GmbH, 2002-2016

Acronis Cloud, you can now store your mobile backups in local storage on your computer. For this operation, you need to have Acronis True Image installed on your computer and the Acronis True Image mobile app installed on your mobile device.

- **Improved user interface**—Due to popular customer requests, the product interface was improved and simplified. This includes sorting backups in the list, adaptation for NAS devices to use as a backup destination, backup encryption indication, and other items.
- **Default sync removal**—You can delete the default sync, as any other ordinary sync. It will not be recreated automatically.
- **Automatic backup destination recognition**—When Windows assigns a different drive letter to the device that you use as a backup destination, the backup settings will not be broken. Acronis True Image recognizes the device and continues the backup without errors.

1.2.1 Alternatives to the removed features

After a detailed review, it was decided to remove a number of outdated and redundant features from Acronis True Image. The following is the list of the features that were removed and alternative ways of performing the same functions and operations in your version of Acronis True Image.

For more information, refer to the Knowledge Base article: https://kb.acronis.com/content/48662.

- **Email backup**. This feature becomes less and less popular, since most of our customers use web-based email systems. Please use disk-level backup instead. Refer to Backing up disks and partitions (p. 41) for details.
- **Local and mixed synchronization**. We recommend that you use cloud-based sync, instead. Acronis Cloud is much more reliable storage than a USB flash drive, an internal hard drive, or an external hard drive. One more important advantage — your data in Acronis Cloud is accessible anytime, anywhere. Refer to Sync creation (p. 104) for details.
- **Backup version consolidation**. You can control the number of your backup versions by specifying it in the backup scheme. Refer to Backup schemes (p. 48) for details.
- Manual backup deletion. You can delete an entire backup, configure automatic cleanup rules, or delete a specific backup version while working in the recovery environment (bootable media). Refer to Deleting backups and backup versions (p. 66) for details.

The following features have been removed, as they were originally designed for Windows XP.

- **Acronis Extended Capacity Manager**. In Windows Vista and later, hard drives of over 3 TB in size are supported by the operating system.
- **Trim SSD**. In Windows 7 and later, trimming SSD is natively integrated in the operating system.

1.3 System requirements and supported media

1.3.1 Minimum system requirements

Acronis True Image requires the following hardware:

- Processor Pentium 1 GHz
- 1 GB RAM
- 1.5 GB of free space on a hard disk
- CD-RW/DVD-RW drive or USB flash drive for bootable media creation
- Screen resolution is 1024 x 768
- Mouse or other pointing device (recommended)

Copyright © Acronis International GmbH, 2002-2016

Other requirements:

- An Internet connection is required for the product activation and all features that use Acronis Cloud, including online backup, cloud archiving, and data synchronization. If your computer is not connected to the Internet, you can activate the product by using another computer that has an Internet connection. Refer to Activating Acronis True Image (p. 11) for details.
- You need to have administrator privileges to run Acronis True Image.

1.3.2 Supported operating systems

Acronis True Image has been tested on the following operating systems:

- Windows XP SP3 (32-bit) *
- Windows 7 SP1 (all editions)
- Windows 8 (all editions)
- Windows 8.1 (all editions)
- Windows 10 (all editions)
- Windows Home Server 2011

* Limited support. Some features may not work properly. For example, Online Dashboard and Archiving.

Acronis True Image also lets you create a bootable CD-R/DVD-R that can back up and recover a disk/partition on a computer running any Intel- or AMD- based PC operating system, including Linux®. Note that the Intel-based Apple Macintosh is not supported.

Warning! Successful recovery is only guaranteed for the supported operating systems. Other operating systems may become unbootable after recovery.

1.3.3 Supported file systems

- FAT16/32
- NTFS
- Ext2/Ext3/Ext4 *
- ReiserFS *

  Note: ReiserFS partitions and disks cannot be backed up to Acronis Cloud.
- Linux SWAP *

* The Ext2/Ext3/Ext4, ReiserFS, and Linux SWAP file systems are supported only for disk or partition backup/recovery operations. You cannot use Acronis True Image for file-level operations with these file systems (file backup, recovery, search, as well as image mounting and file recovering from images). You also cannot perform backups to disks or partitions with these file systems.

If a file system is not supported or is corrupted, Acronis True Image can copy data using a sector-by-sector approach.

Copyright © Acronis International GmbH, 2002-2016

1.3.4 Supported Internet connection types

The table below shows which Internet connection types are supported by the product functions.

	Internet connection type				
	Acronis Console in Windows		Acronis Bootable media		
	Any connection established in Windows	Proxy server	Ethernet cable	Wi-Fi	Proxy server
Disk-level and file-level backup to Acronis Cloud	+	-	-	-	-
Disk-level recovery from Acronis Cloud	+	-	+	+	-
File-level recovery from Acronis Cloud	+	-	-	-	-
Data synchronization	+	-	-	-	-
Product activation	+	- *	-	-	-
Product update	+	- **	-	-	-

* - You can activate the product by using an activation code. Refer to the **Activation from another computer** section in Activating Acronis True Image (p. 11) for details.

** - To update the product, download the newer product version from the Acronis website and install it over your current one.

1.3.5 Supported storage media

- Hard disk drives*
- Solid State Drives (SSD)
- Networked storage devices
- FTP servers**
- CD-R/RW, DVD-R/RW, DVD+R (including double-layer DVD+R), DVD+RW, DVD-RAM, BD-R, BD-RE
- USB 1.1 / 2.0 / 3.0, eSATA, FireWire (IEEE-1394) and PC card storage devices

* Limitations on operations with dynamic disks:

  - Creation of Acronis Secure Zone on dynamic disks is not supported.
  - Recovery of a dynamic volume as a dynamic volume with manual resizing is not supported.
  - Try&Decide® cannot be used for protecting dynamic disks.
  - "Clone disk" operation is not supported for dynamic disks.

** An FTP server must allow passive mode file transfers. Acronis True Image splits a backup into files with a size of 2GB when backing up directly to an FTP server.

The firewall settings of the source computer should have Ports 20 and 21 opened for the TCP and UDP protocols to function. The **Routing and Remote Access** Windows service should be disabled.

Copyright © Acronis International GmbH, 2002-2016

1.4 Installing Acronis True Image

Installing Acronis True Image

To install Acronis True Image:

1. Run the setup file. Before starting the setup process, Acronis True Image will check for a newer build on the website. If there is one, the newer version will be offered for installation.
2. Click **Install**.

   Acronis True Image will be installed on your system partition (usually C:).
3. When the installation is complete, click **Start application**.
4. Read and accept the terms of the license agreements for Acronis True Image and Bonjour.

   Bonjour software will be installed on your computer for advanced support of NAS devices. You can uninstall the software at any time.
5. In the opened window, sign in to your Acronis account. The product will be automatically activated.

   You can skip this step. In this case, enter your serial number, and then click **Activate**.

   Refer to Acronis account (p. 24) for details.

By installing the application, you agree to participate in the Acronis Customer Experience Program. You can change this setting at any time.

Recovering from an Acronis True Image error

If Acronis True Image ceased running or produced errors, its files might be corrupted. To repair this problem, you first have to recover the program. To do this, run Acronis True Image installer again. It will detect Acronis True Image on your computer and will ask you if you want to repair or remove it.

Removing Acronis True Image

Select **Start** -> **Settings** -> **Control panel** -> **Add or remove programs** -> **Acronis True Image** -> **Remove**. Then follow the instructions on the screen. You may have to reboot your computer afterwards to complete the task.

If you use Windows 7, click **Start** -> **Control Panel** -> **Uninstall a program** -> **Acronis True Image** -> **Uninstall**.

If you use Windows 8, click the Settings icon, then select **Control Panel** -> **Uninstall a program** -> **Acronis True Image** -> **Uninstall**.

If you use Windows 10, click **Start** -> **Settings** -> **System** -> **Apps & features** -> **Acronis True Image** -> **Uninstall**.

If you used the Acronis Secure Zone or Acronis Nonstop Backup (p. 35), select in the window that appears what to do with the zone and Nonstop Backup storages.

Upgrading from old versions of Acronis True Image

If your current version of Acronis True Image is Acronis True Image 2015 or Acronis True Image 2016, the new version will simply update it; there is no need to remove the old version and reinstall the software. If your current version is older, we recommend that you remove the current version, first.

Please keep in mind that the backups created by the later program version may be incompatible with the previous program versions. Therefore, if you roll back Acronis True Image to an older version, you

Copyright © Acronis International GmbH, 2002-2016

likely will have to re-create the backups using the older version. We strongly recommend that you create new bootable media after each product upgrade.

1.5 Activating Acronis True Image

To use Acronis True Image, you need to activate it via the Internet. Without activation the fully functional product works for 30 days. If you do not activate it during that period, all the program functions become unavailable except the recovery.

Activating Acronis True Image

You can activate Acronis True Image either on your computer or from another computer, if your computer is not connected to the Internet.

Activation on a computer connected to the Internet

If your computer is connected to the Internet, the product will be activated automatically.

If the computer where you install Acronis True Image does not have Internet connection or if the program cannot connect to Acronis Activation Server, click **Account** on the sidebar, and then select one of the following actions:

- **Try again** - select this option to try to connect to the Acronis Activation Server again.
- **Activate offline** - you can activate the program manually from another computer that is connected to the Internet (see below).

Activation from another computer

If your computer is not connected to the Internet, you may activate Acronis True Image by using another computer which has connection to the Internet.

To activate the product from another computer:

1. On your computer, install and start Acronis True Image.
2. On the sidebar, click **Account**, and then click **Activate offline**.
3. In the Acronis True Image Activation window, perform 3 simple steps:
    1. Save your installation code to a file by clicking the **Save to file** button, and specify a removable media as the file location (for example, a USB flash drive). You may also simply write down this code on a piece of paper.
    2. On another computer which has the Internet connection, go to http://www.acronis.com/activation/. The instructions on the screen will help you to get your activation code by using the installation code. Save the obtained activation code to a file on a removable media, or write it down on paper.
    3. On your computer, click the **Load from file** button and specify a path to the file with the activation code; or, simply type it into the box from the piece of paper.
4. Click **Activate**.

"Too many activations" issue

Possible reasons for the issue:

- **You exceed the maximum number of computers with installed Acronis True Image.**

  For example, you have one license or a serial number for one computer and you install Acronis True Image on a second computer.

  Solutions:

Copyright © Acronis International GmbH, 2002-2016

- Enter a new serial number. If you do not have one, you can buy it in the Acronis built-in store or at the Acronis website.
- Move the license to your new computer from another one on which the product is already activated. To do this, select the computer from which you want to move the license. Note that Acronis True Image will be deactivated on that computer.

- **You reinstall Windows or change hardware of your computer.**

  For example, you might upgrade motherboard or processor in your computer. Activation is lost, because Acronis True Image sees your computer as a new one.

  Solution:

  To reactivate Acronis True Image on your computer, choose from the list the same computer by its old name.

1.6 Trial version information

General limitations

The trial version of Acronis True Image works only during the trial period of 30 days. It has the following limitations:

- Disk cloning is disabled.
- When booting from an Acronis bootable media, the only available operation is recovery.

Synchronization

Data synchronization is available without any limitations, but when the trial period expires:

- Your computer is excluded from all syncs. After activating the full version of Acronis True Image you will be able to connect to the syncs again.
- All the versions of synced files will be permanently deleted from Acronis Cloud.

Acronis Cloud

You have 1000 GB of storage space on the cloud during the trial period. You can use this space to store your online backups, archives, and versions of synced files. After the trial period is over, Acronis Cloud works in recovery-only mode for 30 days. After this period, you won't be able to use the Acronis Cloud service and all your data on the Cloud will be deleted.

Purchasing the full version

You can buy the full version at the Acronis website or using in-app purchase functionality. See details in Upgrading Acronis True Image.

1.7 Upgrading Acronis True Image

If your current version of Acronis True Image is Acronis True Image 2015 or Acronis True Image 2016, the new version will simply update it; there is no need to remove the old version and reinstall the software. If your current version is older, we recommend that you remove the current version, first.

Your backups created with a previous version of Acronis True Image are completely compatible with the newer product version. After you upgrade, all of your backups will automatically be added to your backup list.

We strongly recommend that you create new bootable media after each product upgrade.

Copyright © Acronis International GmbH, 2002-2016

Purchasing the full version while using the trial version

To purchase the full version of the product:

1. Start Acronis True Image.
2. On the sidebar, click **Account**, and then click **Buy full version**. The built-in store opens.
3. Select the license that you want to buy, and then click **Buy now**.
4. Provide your payment information.

Updating Acronis True Image

To update Acronis True Image:

1. Start Acronis True Image.
2. On the sidebar, click **Account**.

   If there is a new version available, you will see the appropriate message next to the current build number.
3. Click **Download and install**.

   Before you start downloading, please make sure that your firewall won't block the download process.
4. When the new version is downloaded, click **Install now**.

To check for updates automatically, go to the **Settings** tab, and then select the **Automatically check for updates at startup** check box.

Built-in store

Acronis True Image provides an in-app store. Using this store, you can:

- Buy the full version of Acronis True Image.
- Buy Acronis True Image subscription.
- Buy more storage space on Acronis Cloud.

To access the in-app store, go to the **Account** tab, and then click **Acronis Store**. You will see the in-app store and all available purchase options.

Installing Acronis hotfixes

Acronis hotfix is a small update for Acronis products. It makes changes to one or more application files or registry keys but does not change an application version. A hotfix targets only a specific Acronis True Image build, and cannot be applied to any other build.

To install an Acronis hotfix, follow the steps described in **Updating Acronis True Image** above. A list of available hotfixes for the current build will be displayed in a table, where you can select those you want to install.

1.8 Technical Support

Maintenance and Support Program

If you need assistance with your Acronis product, please go to http://www.acronis.com/support/

Product Updates

You can download the latest updates for all your registered Acronis software products from our website at any time after logging into your **Account** (http://www.acronis.com/my) and registering

Copyright © Acronis International GmbH, 2002-2016

the product. See **Registering Acronis Products at the Website** (http://kb.acronis.com/content/4834) and **Acronis Website User Guide** (http://kb.acronis.com/content/8128).

Copyright © Acronis International GmbH, 2002-2016

2 Getting started

In this section

User interface language 15
Protecting your system 15
Backing up all data on your PC 18
Backing up your files 19
Cloning your hard drive 21
Recovering your computer 22
Recovering your files and folders 24
Acronis account 24
Getting started with Acronis Cloud 25

2.1 User interface language

Before you start, select a preferred language for the Acronis True Image user interface. By default, the language is set in accordance with your Windows display language.

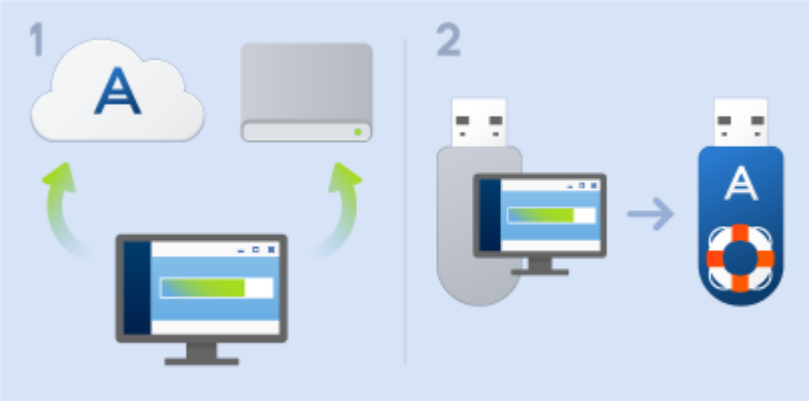
To change the user interface language:

1. Start Acronis True Image.
2. In the **Settings** section, select a preferred language from the list.

2.2 Protecting your system

To protect your system:

1. Back up your computer (p. 16).
2. Create bootable media (p. 17).



It is recommended to test the rescue media as described in Making sure that your rescue media can be used when needed (p. 126).

Copyright © Acronis International GmbH, 2002-2016

2.2.1 Step 1. Backing up your computer

When should I back up my computer?

Create a new backup version after every significant event in your system.

Examples of these events include:

- You bought a new computer.
- You reinstalled Windows on your computer.
- You configured all system settings (for example, time, date, language) and installed all necessary programs on your new computer.
- Important system update.

To ensure you save a healthy state of a disk, it is a good idea to scan it for viruses before backing it up. Please use antivirus software for this purpose. Note this operation often takes a significant amount of time.

How do I create a backup of my computer?

You have two options to protect your system:

- **Entire PC backup (recommended)**

  Acronis True Image backs up all your internal hard drives in disk mode. The backup contains the operating system, installed programs, system settings, and all your personal data including your photos, music, and documents. Refer to Backing up all data on your PC (p. 18) for details.
- **System disk backup**

  You can choose to back up your system partition or the entire system drive. Refer to Backing up disks and partitions (p. 41) for details.

We do not recommend using nonstop backup as a primary way to protect your system, because the main purpose of this technology is protection of frequently changed files. For the safety of your system, use any other schedule. See examples in Examples of custom schemes (p. 51). Refer to Using Acronis Nonstop Backup (p. 35) for more details about the Nonstop Backup feature.

To back up your computer:

1. Start Acronis True Image.
2. On the sidebar, click **Backup**.

   If this is your first backup, you will see the backup configuration screen. If you already have some backups in the backup list, then first click **Add backup**, and then click **Create new backup**.
3. Click the **Backup source** icon, and then select **Entire PC**.

   If you want to back up your system disk only, then click **Disks and partitions**, and then select your system partition (usually C:) and the System Reserved partition (if any).
4. Click the **Backup destination** icon, and then select a storage place for the backup (see recommendation below).
5. Click **Back up now**.

Result: A new backup box appears in the backup list. To create a new version of the backup in future, select the backup box from the list, and then click **Back up now**.

Where do I store my disk backups?

- **Good:** Your ordinary internal hard disk.
- **Better:** Acronis Secure Zone (p. 137). This is a special secure partition on your local hard drive for storing backups.

Copyright © Acronis International GmbH, 2002-2016

- **The best:** Acronis Cloud (p. 25) or an external hard disk.

Refer to Deciding where to store your backups (p. 33) for details.

How many backup versions do I need?

In most cases, you need 2-3 backup versions of your entire PC contents or your system disk, with a maximum of 4-6 (see above for information about when to create backups). **You can control the number of backup versions by using automatic cleanup rules.** Refer to Custom schemes (p. 50) for details.

Remember, the first backup version (the full backup version) is the most important. It is the biggest one, because it contains all data stored on the disk. Further backup versions (the incremental and differential backup versions) may be organized in different schemes. These versions contain only data changes. That's why they are dependent on the full backup version and why the full backup version is so important.

By default, a disk backup is created by using the incremental scheme. This scheme is optimal, in most cases.

For advanced users: it is a good idea to create 2-3 full backup versions and store them on different storage devices. This method is much more reliable.

2.2.2 Step 2. Creating bootable rescue media

What is bootable media?

Bootable media is a product, such as a CD-R/RW or a USB flash drive, from which you can run Acronis True Image when Windows cannot start. You can make a media bootable by using Acronis Media Builder.

How do I create bootable media?

1. Insert a CD-R/RW or plug in a USB flash drive.
2. Start Acronis True Image.
3. On the sidebar, click **Tools**, and then click **Rescue Media Builder**.
4. On the first step, select **Acronis bootable rescue media**.
5. Select the device to use to create the bootable media.
6. Click **Proceed**.

How do I use bootable media?

Use bootable media to recover your computer when Windows cannot start.

1. Connect the bootable media to your computer (insert the CD or plug in the USB drive).
2. Arrange the boot order in BIOS so that your rescue media device (CD or USB drive) is the first device to be booted.

   Refer to Arranging boot order in BIOS (p. 81) for details.
3. Boot your computer from the rescue media and select **Acronis True Image**.

   Result: Once Acronis True Image is loaded, you can use it to recover your computer.

Refer to Acronis Media Builder (p. 122) for details.

Copyright © Acronis International GmbH, 2002-2016

2.3 Backing up all data on your PC

What is an Entire PC backup?

An Entire PC backup is the easiest way to back up the full contents of your computer. We recommend that you choose this option when you are not sure which data that you need to protect. If you want to back up your system partition only, refer to Backing up disks and partitions (p. 41) for details.

When you select Entire PC as a backup type, Acronis True Image backs up all your internal hard drives in disk mode. The backup contains the operating system, installed programs, system settings, and all your personal data including your photos, music, and documents.

The recovery from an Entire PC backup is also simplified. You only need to choose the date to which you want to revert your data. Acronis True Image recovers all data from the backup to the original location. Note that you cannot select specific disks or partitions to recover and you cannot change the default destination. If you need to avoid these limitations, we recommend that you back up your data with an ordinary disk-level backup method. Refer to Backing up disks and partitions (p. 41) for details.

You can also recover specific files and folders from an Entire PC backup. Refer to Backing up files and folders (p. 42) for details.

If an Entire PC backup contains dynamic disks, you recover your data in partition mode. This means that you can select partitions to recover and change recovery destination. Refer to About recovery of dynamic/GPT disks and volumes (p. 79) for details.

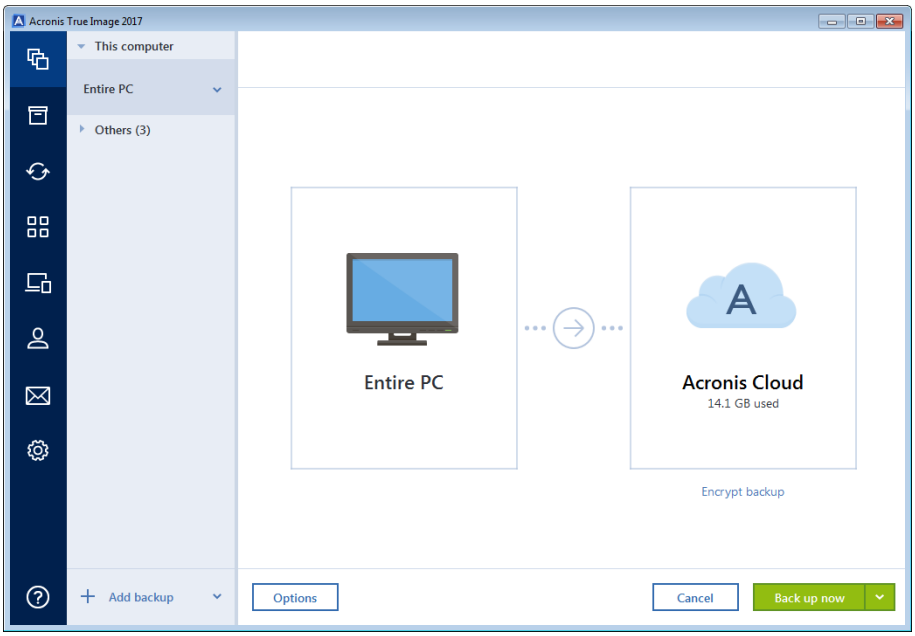
How do I create an Entire PC backup?

To back up the entire contents of your computer:

1. Start Acronis True Image.
2. On the sidebar, click **Backup**.
3. Click the plus sign at the bottom of the backup list.
4. Click the **Backup source** icon, and then select **Entire PC**.
5. Click the **Backup destination** icon, and then select a destination for the backup.

Copyright © Acronis International GmbH, 2002-2016

We recommend that you back up your computer to Acronis Cloud or to local or network storage. Refer to Deciding where to store your backups (p. 33) for details.



6. [optional step] Click **Options** to set the options for the backup, including Schedule (p. 46), Scheme (p. 48), and Password protection (p. 56). For more information see Backup options (p. 44).
7. Click **Back up now**.

When you back up your data to Acronis Cloud, the first backup may take a considerable amount of time to complete. Further backup processes will likely be much faster, because only changes to files will be transferred over the Internet.

2.4 Backing up your files

To protect files such as documents, photos, music files, and video files, there is no need to back up the entire partition containing the files. You can back up specific files and folders and save them to the following storage types:

- **Local or network storage**

  This option is fast and easy. Use it to protect rarely changed files.
- **Acronis Cloud**

  This option is reliable. Use it to protect critical files and files that you want to share between devices or people.

Copyright © Acronis International GmbH, 2002-2016

To use Acronis Cloud, you must have an Acronis account and a subscription to the Acronis Cloud service. Refer to Subscription information (p. 25) for details.

To back up files and folders:

1. Start Acronis True Image.
2. On the sidebar, click **Backup**.
3. Click the **Backup source** icon, and then select **Files and folders**.
4. In the opened window, select the check boxes next to the files and folders that you want to back up, and then click **OK**.
5. Click the **Backup destination** icon, and then select a destination for backup:
   - **Acronis Cloud**—Sign in to your Acronis account, and then click **OK**.
   - **Your external drive**—When an external drive is plugged into your computer, you can select it from the list.
   - **NAS**—Select an NAS from the list of found NAS devices. If you have only one NAS, Acronis True Image will suggest using it as a backup destination by default.
   - **Browse**—Select a destination from the folder tree.
6. Click **Back up now**.

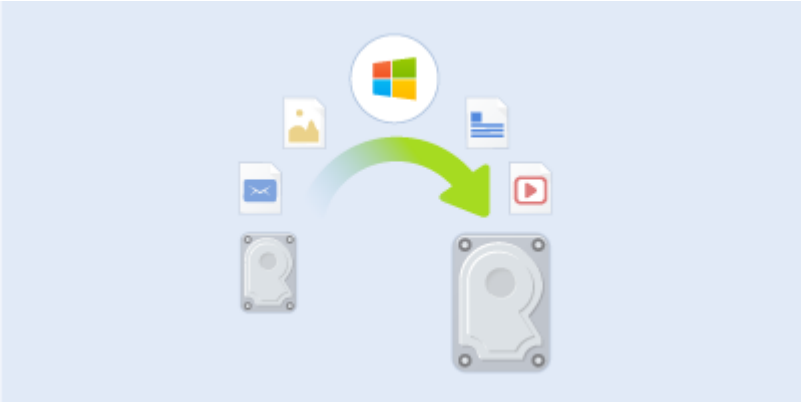
Refer to Backing up files and folders (p. 42) for details.

Copyright © Acronis International GmbH, 2002-2016

2.5 Cloning your hard drive

Why do I need it?

When you see that the free space on your hard drive is not enough for your data, you might want to buy a new, larger hard drive and transfer all your data to the new drive. The usual copy operation does not make your new hard drive identical to the old one. For example, if you open File Explorer and copy all files and folders to the new hard drive, Windows will not start from the new hard drive. The Clone disk utility allows you to duplicate all your data and make Windows bootable on your new hard drive.



Before you start

We recommend that you install the target (new) drive where you plan to use it and the source drive in another location, for example, in an external USB enclosure. This is especially important for laptops.

Warning! Your old and new hard drives must work in the same controller mode (for example, IDE or AHCI). Otherwise, your computer will not start from the new hard drive.

Using the Clone disk utility

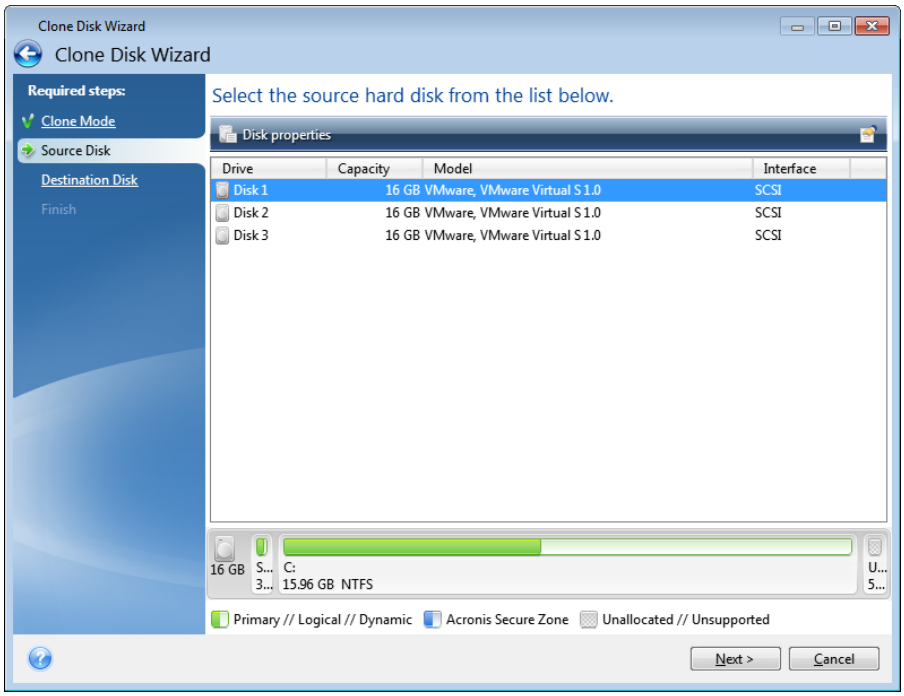
To clone a disk:

1. On the sidebar, click **Tools**, and then click **Clone disk**.
2. On the **Clone Mode** step, we recommend that you choose the **Automatic** transfer mode. In this case, the partitions will be proportionally resized to fit your new hard drive. The **Manual** mode provides more flexibility. Refer to Clone Disk wizard (p. 113) for more details about the manual mode.

   If the program finds two disks, one partitioned and another unpartitioned, it will automatically recognize the partitioned disk as the source disk and the unpartitioned disk as the destination disk. In this case, the next steps will be bypassed and you will be taken to the cloning Summary screen.

Copyright © Acronis International GmbH, 2002-2016

3. On the **Source Disk** step, select the disk that you want to clone.



4. On the **Destination Disk** step, select the destination disk for the cloned data.

   If any disk is unpartitioned, the program will automatically recognize it as the destination and bypass this step.

5. On the **Finish** step, ensure that the configured settings suit your needs, and then click **Proceed**.

By default, Acronis True Image shuts down the computer after the clone process finishes. This enables you to change the position of master/subordinate jumpers and remove one of the hard drives.

2.6 Recovering your computer

Please be aware that recovery of a system disk is an important operation. Before you start, we recommend that you read the detailed descriptions in the following Help topics:

- Trying to determine the crash cause (p. 69)
- Preparing for recovery (p. 70)
- Recovering your system to the same disk (p. 70)

Let's consider two different cases:

1. Windows works incorrectly, but you can start Acronis True Image.
2. Windows cannot start (for example, you turn on your computer and see something unusual on your screen).

Copyright © Acronis International GmbH, 2002-2016

Case 1. How to recover computer if Windows works incorrectly?

1. Start Acronis True Image.
2. On the sidebar, click **Backup**.
3. From the backup list, select the backup that contains your system disk. The backup can be located on local, network storage, or Acronis Cloud.
4. Depending on the backup type, click **Recover PC** or **Recover disks**.
5. In the opened window, select the backup version (the data state from a specific date and time).
6. Select the system partition and the System Reserved partition (if any) to be recovered.
7. Click **Recover now**.

To complete the operation, Acronis True Image must restart your system.

Case 2. How to recover computer if Windows cannot start?

1. Connect Acronis bootable media to your computer, and then run the special standalone version of Acronis True Image.

   Refer to Step 2 Creating bootable rescue media (p. 17) and Arranging boot order in BIOS (p. 81) for details.
2. On the Welcome screen, select **My disks** below **Recover**.
3. Select the system disk backup to be used for recovery. Right-click the backup and choose **Recover**.

   When the backup is not displayed, click **Browse** and manually specify the path to the backup. In the same window, you can connect to Acronis Cloud and select an online backup. Refer to Recovering your system from Acronis Cloud (p. 87) for details.
4. At the **Recovery method** step, select **Recover whole disks and partitions**.

Copyright © Acronis International GmbH, 2002-2016

5. Select the system partition (usually C) on the **What to recover** screen. Note that you may distinguish the system partition by the Pri, Act flags. Select the System Reserved partition (if any), as well.
6. You may leave all settings of the partitions without changes and click **Finish**.
7. Check the summary of operations, and then click **Proceed**.
8. When the operation finishes, exit the standalone version of Acronis True Image, remove the rescue media (if any), and boot from the recovered system partition. After making sure that you have recovered Windows to the state you need, restore the original boot order.

2.7 Recovering your files and folders

You can recover files and folders both from file-level and disk-level backups.

To recover files and folders:

1. Start Acronis True Image.
2. On the sidebar, click **Backup**.
3. From the backup list, select the backup which contains the files or folders that you want to recover.

   The backup can be located on local, network storage, or Acronis Cloud. When you recover data from Acronis Cloud, you first need to sign in to your Acronis account.
4. On the right panel, click **Recover files**.
5. Select the backup version (the data state from a specific date and time).
6. Select the files and folders that you want to recover, and then click **Next**.
7. Select a destination on your computer for the recovered files/folders. You can recover data to its original location or choose a new one, if necessary. To choose a new location, click the **Browse** button.
8. To start the recovery process, click the **Recover now** button.

2.8 Acronis account

An Acronis account is required when you:

- Register an Acronis product.
- Back up to Acronis Cloud.
- Synchronize your data.
- Archive your data.

How to create an Acronis account

If you do not have an Acronis account yet, perform the following steps:

1. On the sidebar, click **Account**, and then click **Sign in or create an account**.
2. Click **Create account**.
3. In the opened registration form, provide your email address, a password for your new account and confirm the password by retyping it once more in the appropriate field.

   To keep your personal data secure, choose a strong password for your online backups, guard it from getting into the wrong hands, and change it from time to time.
4. Click **Create account**.

Copyright © Acronis International GmbH, 2002-2016

5. An email message will be sent to the address you specified. Open this message and confirm your wish to create an account.

How to sign in

To sign in to your Acronis account:

1. On the sidebar, click **Account**, and then click **Sign in** or create an account.
2. Enter your registration email address and password, and then click **Sign in**.

How to sign out

To sign out of your Acronis account:

1. On the sidebar, click **Account**.
2. Click your email address, and then choose **Sign out**.

2.9 Getting started with Acronis Cloud

Acronis Cloud might be unavailable in your region. For more information, click here: http://kb.acronis.com/content/4541

Remote storage

On the one hand, Acronis Cloud is a secure remote storage which you can use to store:

- Backups of your files and folders
- Backups of your partitions and disks
- Versions of your synchronized files and folders
- Archives

Because files are stored on a remote storage, they are protected even if your computer is stolen or your house burns down. In the case of a disaster or data corruption, you can recover your files and even the entire contents of your computer.

With one account, you can save data from several computers and all your mobile devices running iOS and Android operating systems. Refer to Acronis True Image for mobile devices (p. 109) for details.

To start using Acronis Cloud, you need a subscription to the service. Refer to Subscription information (p. 25) for details.

Web application

On the other hand, Acronis Cloud is a web application that allows you to recover and manage the data you store on Acronis Cloud. To work with the application, you can use any computer connected to the Internet.

To access the application, go to https://www.acronis.com/my/online-backup/, log in to your account, and then click **Recover my data now**.

2.9.1 Subscription information

Performing backups to Acronis Cloud requires subscription to the Acronis Cloud service. To subscribe, start Acronis True Image and sign in using your Acronis account. Refer to Acronis account (p. 24) for details.

Copyright © Acronis International GmbH, 2002-2016

Please note that Acronis Cloud is subject to our Fair Usage Policy. See more details at: https://kb.acronis.com/ati2017/fairusage.

Trial version

When you activate the trial version of the product, a 1000 GB storage and 30-day free subscription to Acronis Cloud is assigned to your account automatically. See details in Trial version information (p. 12).

Full version

You can purchase the full Acronis Cloud subscription in the **Account** section of your version of Acronis True Image or at the Acronis website. See details in Upgrading Acronis True Image.

Copyright © Acronis International GmbH, 2002-2016

3 Basic concepts

In this section

Basic concepts 27
The difference between file backups and disk/partition images 28
Full, incremental and differential backups 29
FAQ about backup, recovery and cloning 31
Deciding where to store your backups 33
Using Acronis Nonstop Backup 35
Backup file naming 37
Integration with Windows 38
Wizards 39

3.1 Basic concepts

This section provides general information about basic concepts which could be useful for understanding how the program works.

Backup and recovery

Backup refers to the making copies of data so that these additional copies may be used to **recover** the original after a data loss event.

Backups are useful primarily for two purposes:

- To recover an operating system when it is corrupted or cannot start (called disaster recovery). Refer to Protecting your system (p. 15) for more details about protecting your computer from a disaster.
- To recover specific files and folders after they have been accidentally deleted or corrupted.

Acronis True Image does both by creating disk (or partition) images and file-level backups respectively.

Backup versions

Backup versions are the file or files created during each backup operation. The number of versions created is equal to the number of times the backup is executed. So, a version represents a point in time to which the system or data can be restored.

Backup versions represent full, incremental and differential backups - see Full, incremental and differential backups (p. 29).

The backup versions are similar to file versions. The file versions concept is familiar to those who use a Windows feature called "Previous versions of files". This feature allows you to restore a file as it existed on a particular date and time. A backup version allows you to recover your data in a similar way.

Disk cloning

This operation copies the entire contents of one disk drive to another disk drive. This may be necessary, for example, when you want to clone your operating system, applications, and data to a new larger capacity disk. You can do it two ways:

- Use the Clone disk utility.

Copyright © Acronis International GmbH, 2002-2016

- Back up your old disk drive, and then recover it to the new one.

Backup file format

Acronis True Image usually saves backup data in the proprietary tib format using compression. The data from .tib file backups can be recovered only through Acronis True Image, in Windows or in the recovery environment.

Acronis Nonstop Backup uses a special hidden storage for data and metadata. The backed up data is compressed and split into files of about 1 GB. These files also have a proprietary format and the data they contain can be recovered only with the help of Acronis True Image.

Backup validation

The backup validation feature allows you to confirm that your data can be recovered. The program adds checksum values to the data blocks being backed up. During backup validation, Acronis True Image opens the backup file, recalculates the checksum values and compares those values with the stored ones. If all compared values match, the backup file is not corrupted.

Scheduling

For your backups to be really helpful, they must be as "up-to-date" as possible. Schedule your backups to run automatically and on a regular basis.

Deleting backups

When you want to delete backups and backup versions you no longer need, please do it by using the tools provided by Acronis True Image. Refer to Deleting backups and backup versions (p. 66) for details.

Acronis True Image stores information on the backups in a metadata information database. Therefore, deleting unneeded backup files in File Explorer will not delete information about these backups from the database. This will result in errors when the program tries to perform operations on the backups that no longer exist.

3.2 The difference between file backups and disk/partition images

When you back up files and folders, only the files and folder tree are compressed and stored.

Disk/partition backups are different from file and folder backups. Acronis True Image stores an exact snapshot of the disk or partition. This procedure is called "creating a disk image" or "creating a disk backup" and the resulting backup is often called "a disk/partition image" or "a disk/partition backup".

What does a disk/partition backup contain?

A disk/partition backup contains all the data stored on the disk or partition:

1. Zero track of the hard disk with the master boot record (MBR) (applicable to MBR disk backups only).
2. One or more partitions, including:
    1. Boot code.
    2. File system meta data, including service files, file allocation table (FAT), and partition boot record.

Copyright © Acronis International GmbH, 2002-2016

3. File system data, including operating system (system files, registry, drivers), user data and software applications.
3. System Reserved partition, if any.
4. EFI system partition, if any (applicable to GPT disk backups only).

What is excluded from disk backups?

To reduce image size and speed up image creation, by default Acronis True Image only stores the hard disk sectors that contain data.

Acronis True Image excludes the following files from a disk backup:

- pagefile.sys
- hiberfil.sys (a file that keeps RAM contents when the computer goes into hibernation)

You can change this default method by turning on the sector-by-sector mode. In this case, Acronis True Image copies all hard disk sectors, and not only those that contain data.

Additionally, when you back up your system partition or disk to Acronis Cloud, Acronis True Image excludes the following data:

- The Temp folders, usually located in:
  - C:\Windows\Temp\
  - C:\Users\<username>\AppData\Local\Temp
- The System Volume Information folder (usually located in C:\System Volume Information\)
- The Recycle Bin
- Web browser temporary data:
  - Temporary Internet files
  - Cookies
  - History
  - Cache
- .tib files
- .tmp files
- .~ files

3.3 Full, incremental and differential backups

Acronis True Image offers three backup methods:

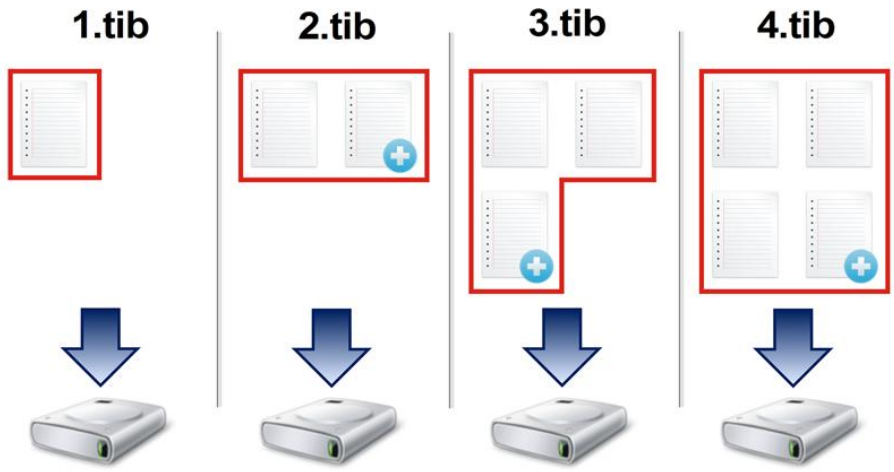
Full method

The result of a full method backup operation (also known as full backup version) contains all of the data at the moment of the backup creation.

Example: Every day, you write one page of your document and back it up using the full method. Acronis True Image saves the entire document every time you run backup.

Copyright © Acronis International GmbH, 2002-2016

1.tib, 2.tib, 3.tib, 4.tib - full backup versions.



Additional information

A full backup version forms a base for further incremental or differential backups. It can also be used as a standalone backup. A standalone full backup might be an optimal solution if you often roll back the system to its initial state or if you do not like to manage multiple backup versions.

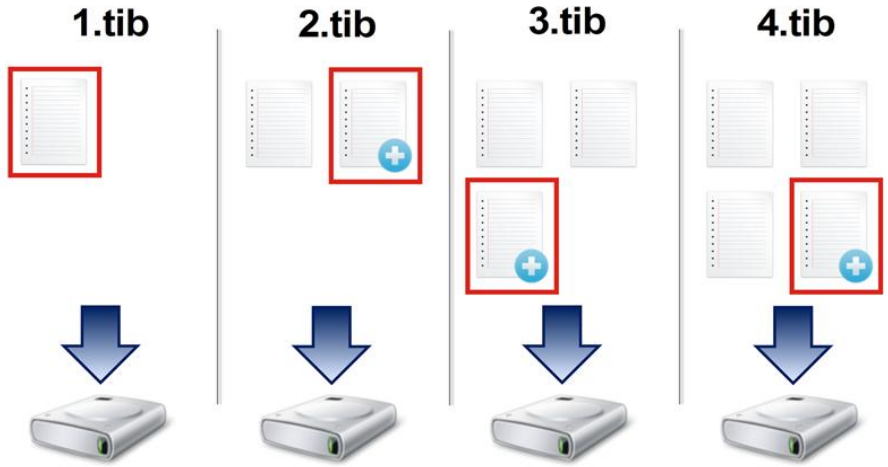
Incremental method

The result of an incremental method backup operation (also known as incremental backup version) contains only those files which have been changed since the LAST BACKUP.

Example: Every day, you write one page of your document and back it up using the incremental method. Acronis True Image saves the new page every time you run backup.

Note: The first backup version you create always uses full method.

- 1.tib - full backup version.
- 2.tib, 3.tib, 4.tib - incremental backup versions.



Additional information

Incremental method is the most useful when you need frequent backup versions and the ability to roll back to a specific point in time. As a rule, incremental backup versions are considerably smaller than full or differential versions.

Copyright © Acronis International GmbH, 2002-2016

On the other hand, incremental versions require more work for the program to provide recovery. In the example above, to recover the entire work from 4.tib file, Acronis True Image reads data from all backup versions. Therefore, if you lose an incremental backup version or it becomes corrupted, all later incremental versions are unusable.

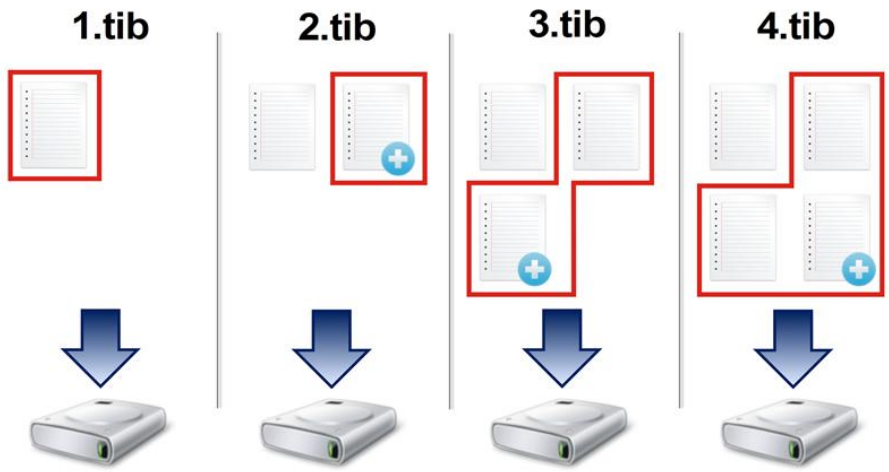
Differential method

The result of a differential method backup operation (also known as differential backup version) contains only those files which have been changed since the LAST FULL BACKUP.

Example: Every day, you write one page of your document and back it up using the differential method. Acronis True Image saves the entire document except the first page stored in the full backup version.

Note: The first backup version you create always uses full method.

- 1.tib - full backup version.
- 2.tib, 3.tib, 4.tib - differential backup versions.



Additional information

Differential method is an intermediate between the first two approaches. It takes less time and space than "Full", but more than "Incremental". To recover data from a differential backup version, Acronis True Image needs only the differential version and the last full version. Therefore, recovery from a differential version is simpler and more reliable than recovery from an incremental one.

An incremental or differential backup created after a disk is defragmented might be considerably larger than usual. This is because the defragmentation program changes file locations on the disk and the backups reflect these changes. Therefore, it is recommended that you re-create a full backup after disk defragmentation.

To choose a desired backup method, you usually need to configure a custom backup scheme. For more information see Custom schemes (p. 50).

3.4 FAQ about backup, recovery and cloning

- **I have a 150GB system partition, but the occupied space on that partition is only 80GB. What will Acronis True Image include in a backup?** - By default, Acronis True Image copies only the hard disk sectors that contain data, so it will include only 80GB in a backup. You can also choose the sector-by-sector mode. Note than such a backup mode is required only in special cases. For more information, see Image creation mode (p. 56). While creating a sector-by-sector backup,

Copyright © Acronis International GmbH, 2002-2016

the program copies both used and unused hard disk sectors and the backup file will usually be significantly larger.

- **Will my system disk backup include drivers, documents, pictures, etc.?** - Yes, such a backup will contain the drivers, as well as the contents of the My documents folder and its subfolders, if you kept the default location of the My documents folder. If you have just a single hard disk in your PC, such a backup will contain all of the operating system, applications and data.
- **I have an old hard disk drive which is almost full in my notebook. I purchased a new bigger HDD. How can I transfer Windows, programs and data to the new disk?** - You can either clone the old hard disk on the new one or back up the old hard disk and then recover the backup to a new one. The optimum method usually depends on your old hard disk partitions layout.
- **I want to migrate my old system hard disk to an SSD. Can this be done with Acronis True Image?** - Yes, Acronis True Image provides such a function. For procedure details, see Migrating your system from an HDD to an SSD (p. 118)
- **What is the best way to migrate the system to a new disk: cloning or backup and recovery?** - The backup and recovery method provides more flexibility. In any case, we strongly recommend to make a backup of your old hard disk even if you decide to use cloning. It could be your data saver if something goes wrong with your original hard disk during cloning. For example, there were cases when users chose the wrong disk as the target and thus wiped their system disk. In addition, you can make more than one backup to create redundancy and increase security.
- **What should I back up: a partition or the whole disk?** - In most cases, it is better to back up the whole disk. However, there may be some cases when a partition backup is advisable. For example, your notebook has a single hard disk with two partitions: system (disk letter C) and the data (disk letter D). The system partition stores your working documents in the My documents folder with subfolders. The data partition stores your videos, pictures, and music files. Such files are already compressed and backing them up using Acronis True Image would not give you significant reduction of the backup file size. However, we recommend creating at least one whole disk backup if your backup storage has enough space.
- **Could you tell me how to clone: in Windows or after booting from the rescue media?** Even when you start cloning in Windows, the computer will reboot into the Linux environment the same as when booting from the rescue media. Because of this, it is better to clone under rescue media. For example, there may be a case when your hard disk drives are detected in Windows and not detected in Linux. If this is the case, the cloning operation will fail after reboot. When booting from the rescue media, you can make sure that Acronis True Image detects both the source and target disks before starting the cloning operation.
- **Can I clone or back up and recover a dual boot machine?** Yes, this is possible when both operating systems are Windows. If your systems are installed in separate partitions of the same physical hard disk drive, cloning or recovery usually proceeds without any problems. If the systems are on different physical hard disk drives, there may be some problems with bootability after recovery.
- **Does Acronis True Image support RAID?** - Acronis True Image supports hardware RAID arrays of all popular types. Support of software RAID configurations on dynamic disks is also provided. Acronis Bootable Rescue Media supports most of the popular hardware RAID controllers. If the standard Acronis rescue media does not "see" the RAID as a single volume, the media does not have the appropriate drivers. In this case you can try to create WinPE-based rescue media. This media may provide the necessary drivers.

 Copyright © Acronis International GmbH, 2002-2016

3.5 Deciding where to store your backups

Acronis True Image supports quite a few of storage devices. For more information, refer to Supported storage media.

The table below shows possible backup destinations for your data.

	HDD (internal or external)	SSD	USB flash drive	Acronis Cloud	File server, NAS or NDAS	Network share	SMB/ NFS share	FTP server	DVD or Blue-ray disc	Memory card
MBR partitions or entire disks (HDD, SSD)	+	+	+	+	+	+	+	+	+	+
GPT/dynamic volumes or disks	+	+	+	+	+	+	+	+	+	+
Files and folders	+	+	+	+	+	+	+	+	+	+

Though backing up to your local hard drive is the simplest option, we recommend that you store your backups off-site because it enhances the security of your data.

Recommended storage media:

1. **Acronis Cloud**
2. **External drive**

   If you plan to use an external USB hard drive with your desktop PC, we recommend that you connect the drive to a rear connector by using a short cable.
3. **Home file server, NAS, or NDAS**

   Please check whether Acronis True Image detects the selected backup storage, both in Windows and when booted from the rescue media.

   To gain access to an NDAS-enabled storage device, in many cases you will need to specify the NDAS device ID (20 characters) and the write key (five characters). The write key allows you to use an NDAS-enabled device in write mode (for example, for saving your backups). Usually the device ID and write key are printed on a sticker attached to the bottom of the NDAS device or on the inside of its enclosure. If there is no sticker, you need to contact your NDAS device vendor to obtain that information.
4. **Network share**

   See also: Authentication settings (p. 35).
5. **FTP server**

   See also: FTP connection (p. 34).
6. **Optical discs (CD, DVD, BD)**

   Blank optical discs such as DVD-R, DVD+R are very cheap, so they will be the lowest cost solution for backing up your data, though the slowest one.

   Due to the necessity of swapping discs, we strongly recommend to avoid backing up to DVDs if the number of discs is more than three. When there is no alternative to backing up to DVDs, we recommend to copy all DVDs to a folder on a hard disk, and then to recover from that folder.

Copyright © Acronis International GmbH, 2002-2016

3.5.1 Preparing a new disk for backup

A new internal or external hard drive may not be recognized by Acronis True Image. If this is the case, use the operating system tools to change the disk status to **Online** and then to initialize the disk.

To change a disk status to Online:

1. Open **Disk Management**. To do this, go to **Control Panel** -> **System and Security** -> **Administrative Tool**, start **Computer Management**, and then click **Disk Management**.
2. Find the disk marked as **Offline**. Right-click the disk and then click **Online**.
3. The disk status will be changed to **Online**. After that, you will be able to initialize the disk.

To initialize a disk:

1. Open **Disk Management**. To do this, go to **Control Panel** -> **System and Security** -> **Administrative Tool**, start **Computer Management**, and then click **Disk Management**.
2. Find the disk marked as **Not Initialized**. Right-click the disk and then click **Initialize Disk**.
3. Select a partition table for the disk - MBR or GPT, and then click **OK**.
4. [optional step] To create a volume on the disk, right-click the disk, click **New Simple Volume**, and then follow the wizard's steps to configure the new volume. To create one more volume, repeat this operation.

3.5.2 FTP connection

Acronis True Image allows you to store your backups on FTP servers.

To create a new FTP connection, when selecting a backup storage click **FTP connection**, and in the opened window provide:

- Path to the FTP server, for example: *my.server.com*
- Port
- User name
- Password

To check your settings, click the **Test connection** button. The computer will try to connect to the specified FTP server. If the test connection has been established, click the **Connect** button to add the FTP connection.

The created FTP connection will appear in the folder tree. Select the connection and browse for the backup storage that you want to use.

Please, be aware that the mere opening of an FTP server's root folder does not bring you to your home directory.

Acronis True Image splits a backup into files with a size of 2GB when backing up directly to an FTP server. If you back up to a hard disk with the aim of transferring the backup to an FTP later, split the backup into files of 2GB each by setting the desired file size in the backup options. Otherwise, the recovery will not be possible.

An FTP server must allow passive mode file transfers.

*The firewall settings of the source computer should have Ports 20 and 21 opened for the TPC and UDP protocols to function. The **Routing and Remote Access** Windows service should be disabled.*

Copyright © Acronis International GmbH, 2002-2016

3.5.3 Authentication settings

If you are connecting to a networked computer, in most cases you will need to provide the necessary credentials for accessing the network share. For example, this is possible when you select a backup storage. The **Authentication Settings** window appears automatically when you select a networked computer name.

If necessary, specify the user name and password, and then click **Test connection**. When the test is successfully passed, click **Connect**.

Troubleshooting

When you create a network share that you plan to use as a backup storage, please ensure that at least one of the following conditions is met:

- Windows account has a password on the computer where the shared folder is located.
- Password-protected sharing is turned off in Windows.

  You can find this setting at **Control Panel** —> **Network and Internet** —> **Network and Sharing Center** —> **Advanced sharing settings** —> Turn off password protected sharing.

Otherwise, you will not be able to connect to the shared folder.

3.6 Using Acronis Nonstop Backup

Acronis Nonstop Backup provides easy protection of your disks and files. It allows you to recover entire disks, individual files and their different versions.

The main purpose of Acronis Nonstop Backup is continuous protection of your data (files, folders, contacts, etc.), though you can use it to protect partitions as well. If you choose to protect an entire partition, you will be able to recover the partition as a whole using the image recovery procedure.

We do not recommend using nonstop backup as a primary way to protect your system. For the safety of your system, use any other schedule. See examples in Examples of custom schemes (p. 51).

Nonstop Backup limitations

- You can create only one nonstop backup.
- Windows libraries (Documents, Music, etc.) can be protected with a disk-level nonstop backup only.
- You cannot protect data stored on external hard drives.
- Nonstop Backup and Try&Decide cannot work simultaneously.

How it works

Once you start Acronis Nonstop Backup, the program will perform an initial full backup of the data selected for protection. Acronis Nonstop Backup will then continually monitor the protected files (including open ones). Once a modification is detected, the changed data is backed up. The shortest interval between the incremental backup operations is five minutes. This allows you to recover your system to an exact point in time.

Acronis Nonstop Backup checks file changes on the disk, not in the memory. If, for instance, you are working in Word and do not use the "Save" operation for a long time, your current changes in the Word document will not be backed up.

Copyright © Acronis International GmbH, 2002-2016

You may think that at these backup rates the storage will fill in no time. Do not worry as Acronis True Image will back up only so called "deltas". This means that only differences between old and new versions will be backed up and not whole changed files. For example, if you use Microsoft Outlook or Windows Mail, your pst file may be very large. Furthermore, it changes with each received or sent E-mail message. Backing up the entire pst file after each change would be an unacceptable waste of your storage space, so Acronis True Image backs up only its changed parts in addition to the initially backed up file.

Retention rules

Acronis Nonstop Backup keeps all backups for the last 24 hours. The older backups will be consolidated in such a way that Nonstop Backup will keep daily backups for the last 30 days and weekly backups until all Nonstop Backup data destination space is used.

The consolidation will be performed every day between midnight and 01:00 AM. The first consolidation will take place after the Nonstop Backup has been working for at least 24 hours. For example, you have turned on the Nonstop Backup at 10:00 AM on July 12. In this case the first consolidation will be performed between 00:00 and 01:00 AM on July 14. Then the program will consolidate the data every day at the same time. If your computer is turned off between 00:00 and 01:00 AM, the consolidation will start when you turn the computer on. If you turn off Nonstop Backup for some time, the consolidation will start after you turn it on again.

3.6.1 Acronis Nonstop Backup data storage

Acronis Nonstop Backup data storage can be created on local hard disk drives (both internal and external).

In many cases an external hard disk will be the best choice for Nonstop Backup data storage. You can use an external disk with any of the following interfaces: USB (including USB 3.0), eSATA, FireWire, and SCSI.

You can also use an NAS as the storage, but with one limitation - it must be accessible with the SMB protocol. It does not matter whether an NAS share you want to use for the storage is mapped as a local disk or not. If the share requires login, you will need to provide the correct user name and password. For more information see Authentication settings (p. 35). Acronis True Image remembers the credentials and the subsequent connections to the share do not require login.

When an external hard disk or NAS is unavailable, the Nonstop Backup destination can be an internal disk, including a dynamic one. Please note that you cannot use a partition to be protected as a Nonstop Backup storage. If your computer has a single hard disk drive with a single partition, but you want to use Acronis Nonstop Backup anyway, you can create Acronis Secure Zone and use it as the Nonstop Backup data storage.

Before creating Acronis Nonstop Backup data storage, Acronis True Image checks whether the selected destination has enough free space. It multiplies the volume of data to be protected by 1.2 and compares the calculated value with the available space. If the free space on the destination satisfies this minimum storage size criterion, the destination can be used for storing Nonstop Backup data.

3.6.2 Nonstop Backup - Frequently asked questions

Why does Acronis Nonstop Backup pause on its own? - This is the designed behavior of Acronis Nonstop Backup. When the system load rises to a critical level, Acronis Nonstop Backup receives the overload alarm from Windows and pauses itself. This is done to aid Windows relieve the load caused

Copyright © Acronis International GmbH, 2002-2016

by other applications. The overload can be caused by running resource-intensive applications (for example, performing a deep system scan with your antivirus software).

In such a case Nonstop Backup automatically pauses and you cannot restart it. After pausing, Acronis Nonstop Backup gives the system one hour to relieve the load and then attempts to restart.

The automatic restart count for Acronis Nonstop Backup is 6. This means that after the first automatic restart Acronis Nonstop Backup will attempt to restart five more times with intervals of exactly one hour between attempts.

After the sixth unsuccessful attempt, Acronis Nonstop Backup will wait for the next calendar day. On the next day the automatic restart count will automatically reset. When not interfered with, Acronis Nonstop Backup performs six restart attempts per day.

The restart attempt count can be reset by doing any of the following:

- Restarting Acronis Nonstop Backup service;
- Rebooting the computer.

Restarting Acronis Nonstop Backup service will only reset the restart count to 0. If the system is still overloaded, Acronis Nonstop Backup will pause again. An Acronis Support Knowledge Base article at http://kb.acronis.com/content/14708 describes the procedure for restarting the Acronis Nonstop Backup service.

Rebooting the computer will reset the load and the restart count. If the system overloads again, Acronis Nonstop Backup will pause.

Why does Acronis Nonstop Backup sometimes cause a high CPU load? - This is the expected behavior of Acronis Nonstop Backup. This may happen on restart of a paused Acronis Nonstop Backup if a considerable amount of protected data has been modified during the pause.

For example, if you manually pause the Acronis Nonstop Backup that you use for protecting your system partition and then install a new application. When you restart Acronis Nonstop Backup, it loads the CPU for some time. However, the process (afcdpsrv.exe) then goes back to normal.

This happens because Acronis Nonstop Backup needs to check the backed up data against the data that have been modified during the pause to ensure protection continuity. If there was a considerable amount of data modified, the process may load CPU for some time. After the check is done and all the modified data is backed up, Acronis Nonstop Backup goes back to normal.

Can I have Acronis Nonstop Backup storage on an FAT32 partition of a local hard disk? - Yes, FAT32 and NTFS partitions can be used as the storage.

Can I set up Acronis Nonstop Backup storage on a network share or NAS? - Yes, Acronis Nonstop Backup supports network shares, mapped drives, NAS and other network attached devices with one limitation - they must use the SMB protocol.

3.7 Backup file naming

A backup file name has the following attributes:

- Backup name
- Backup method (full, inc, diff: full, incremental, differential)
- Number of backup chain (p. 167) (in the form of b#)
- Number of backup (p. 167)version (p. 167)(in the form of s#)

Copyright © Acronis International GmbH, 2002-2016

- Number of volume (in the form of v#)

  For example this attribute changes when you split a backup into several files. Refer to Backup splitting (p. 57) for details.

Thus a backup name may look the following way:

1. **my_documents_full_b1_s1_v1.tib**
2. **my_documents_full_b2_s1_v1.tib**
3. **my_documents_inc_b2_s2_v1.tib**
4. **my_documents_inc_b2_s3_v1.tib**

If you are creating a new backup, and there is already a file with the same name, the program does not delete the old file, but adds to the new file the "-number" suffix, for example, **my_documents_inc_b2_s2_v1-2.tib**.

3.8 Integration with Windows

During installation Acronis True Image provides closer integration with Windows. Such merging allows you to get the most out of your computer.

Acronis True Image integrates the following components:

- Acronis items on the Windows **Start** menu
- Acronis True Image button on the taskbar
- Shortcut menu commands

Windows Start menu

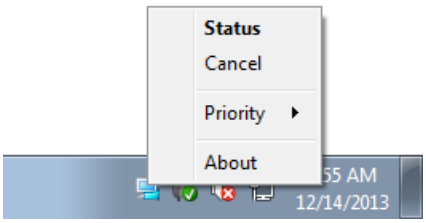
The **Start** menu displays Acronis commands, tools and utilities. They give you access to Acronis True Image functionality, without having to start the application.

Acronis True Image button on the taskbar

The Acronis True Image button on the Windows taskbar shows the progress and result of Acronis True Image operations.

Taskbar notification area icons

During most of the operations, special indicator icons appear in the Windows taskbar notification area. This icon doesn't depend on the main program window being open.



- To view a tooltip indicating the operation's progress or state, point to the icon.
- To view status, change priority or cancel a current operation, right-click the icon, and then click the corresponding command.

Copyright © Acronis International GmbH, 2002-2016

Shortcut menu commands

To access shortcut menu commands, open File Explorer, right-click selected items, point to **Acronis True Image**, and then select a command.

- To create a new file-level backup, select **New file backup**.
- To create a new disk-level backup, select **New disk backup**.
- To mount a disk-level backup (.tib file), select **Mount**.
- To validate a backup (.tib file), select **Validate**.

File-level recovery in File Explorer

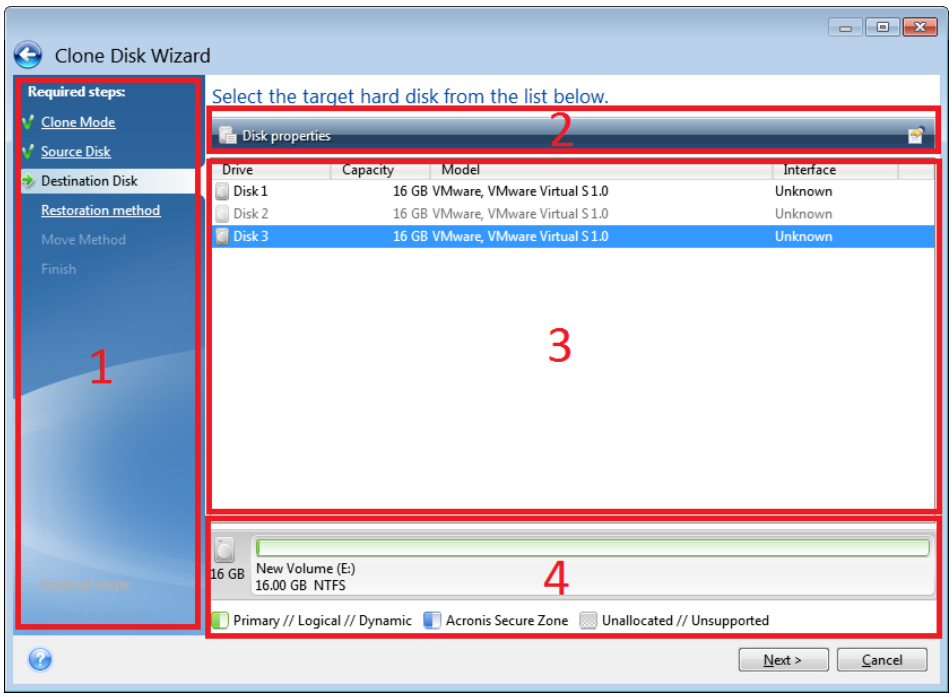
To recover files and folders:

1. In File Explorer, double-click the backup file (.tib file) that contains the data to recover.
2. Copy or drag the files and folders to any location on your computer, as if they were stored on an ordinary disk.

3.9 Wizards

When you use the available Acronis True Image tools and utilities, the program will in many cases employ wizards to guide you through the operations.

For example, see the screen shot below.



A wizard window usually consists of the following areas:

1. This is the list of steps to complete the operation. A green checkmark appears next to a complete step. The green arrow indicates the current step. When complete all the steps, the program displays the Summary screen in the **Finish** step. Check the summary and click **Proceed** to start the operation.
2. This toolbar contains buttons to manage objects you select in area 3.

   For example:

Copyright © Acronis International GmbH, 2002-2016

- **Details** - displays the window that provides detailed information about the selected backup.
- **Properties** - displays the selected item properties window.
- **Create new partition** - displays the window where you can configure a new partition settings.
- **Columns** - allows you to choose which table columns to display and in which order.

3. This is the main area where you select items and change settings.
4. This area displays additional information about the item you select in area 3.

Copyright © Acronis International GmbH, 2002-2016

4 Backing up data

In this section

Backing up disks and partitions.....41
Backing up files and folders 42
Backing up mobile devices 43
Backup options.....44
Operations with backups 63

4.1 Backing up disks and partitions

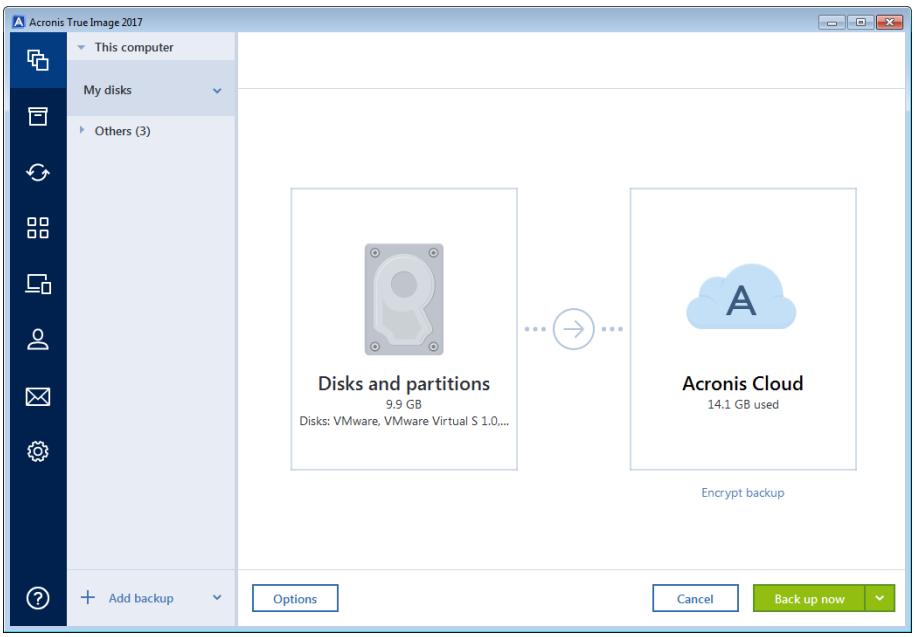
As opposed to file backups, disk and partition backups contain all the data stored on the disk or partition. This backup type is usually used to create an exact copy of a system partition of the whole system disk. Such backup allows you to recover your computer when Windows works incorrectly or cannot start.

To back up partitions or disks:

1. Start Acronis True Image.
2. On the sidebar, click **Backup**.
3. Click **Add backup**.
4. [Optional] To rename the backup, click the arrow next to the backup name, click **Rename**, and then enter a new name.
5. Click the **Backup source** area, and then select **Disks and partitions**.
6. In the opened window, select the check boxes next to the partitions and disks that you want to back up, and then click **OK**.

   To view hidden partitions, click **Full partition list**.

   To back up dynamic disks you can use only the partition mode.



7. Click the **Backup destination** area, and then select a destination for backup:

Copyright © Acronis International GmbH, 2002-2016

- **Acronis Cloud**—Sign in to your Acronis account, and then click **OK**.

  If you do not have an Acronis account, click **Create account**, type your email address, password, and then click the **Create account** button. Refer to Acronis account (p. 24) for details.
- **Your external drive**—When an external drive is plugged into your computer, you can select it from the list.
- **NAS**—Select an NAS from the list of found NAS devices. If you have only one NAS, Acronis True Image will suggest using it as a backup destination by default.
- **Browse**—Select a destination from the folder tree.

If possible, avoid storing your system partition backups on dynamic disks, because the system partition is recovered in the Linux environment. Linux and Windows work with dynamic disks differently. This may result in problems during recovery.

8. [optional step] Click **Options** to set the options for the backup, including Schedule (p. 46), Scheme (p. 48), and Password protection (p. 56). For more information see Backup options (p. 44).
9. [optional step] Click the **Add a comment** icon, and then type a comment to the backup version. Backup comments will help you to find the necessary version later, when recovering your data.
10. Perform one of the following:
    - To run the backup immediately, click **Back up now**.
    - To run the backup later or on a schedule, click the arrow to the right of the **Back up now** button, and then click **Later**.

When you back up your data to Acronis Cloud, the first backup may take a considerable amount of time to complete. Further backup processes will likely be much faster, because only changes to files will be transferred over the Internet.

Once an online backup is started, you are free to close Acronis True Image. The backup process will continue in background mode. If you suspend the backup, turn off your computer, or disconnect it from the Internet, the backup will resume when you click Back up now or when the Internet connection is restored. A backup interruption does not cause your data to be uploaded twice.

4.2 Backing up files and folders

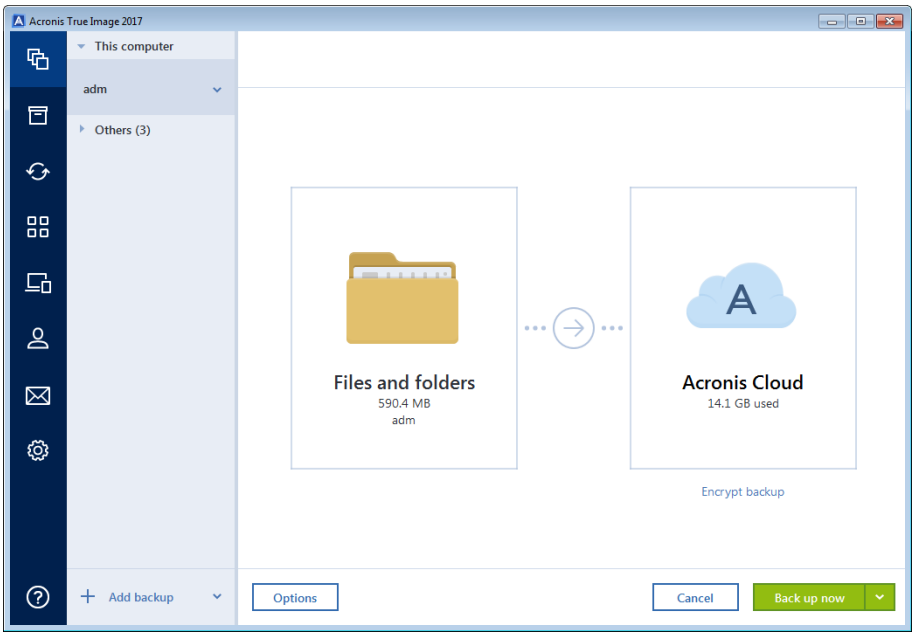
To protect files such as documents, photos, music files, video files, there is no need to back up the entire partition containing the files. You can back up specific files and folders.

To back up files and folders:

1. Start Acronis True Image.
2. On the sidebar, click **Backup**.
3. Click **Add backup**.
4. [Optional] To rename the backup, click the arrow next to the backup name, click **Rename**, and then enter a new name.
5. Click the **Backup source** area, and then select **Files and folders**.

Copyright © Acronis International GmbH, 2002-2016

6. In the opened window, select the check boxes next to the files and folders that you want to back up, and then click **OK**.



7. Click the **Backup destination** area, and then select a destination for backup:
   - **Acronis Cloud**—Sign in to your Acronis account, and then click **OK**.

     If you do not have an Acronis account, click **Create account**, type your email address, password, and then click the **Create account** button. Refer to Acronis account (p. 24) for details.
   - **Your external drive**—When an external drive is plugged into your computer, you can select it from the list.
   - **NAS**—Select an NAS from the list of found NAS devices. If you have only one NAS, Acronis True Image will suggest using it as a backup destination by default.
   - **Browse**—Select a destination from the folder tree.
8. [optional step] Click **Options** to set the options for the backup, including Schedule (p. 46), Scheme (p. 48), and Password protection (p. 56). For more information see Backup options (p. 44).
9. [optional step] Click the **Add a comment** icon, and then type a comment to the backup version. Backup comments will help you to find the necessary version later, when recovering your data.
10. Perform one of the following:
    - To run the backup immediately, click **Back up now**.
    - To run the backup later or on a schedule, click the down arrow to the right of the **Back up now** button, and then click **Later**.

When you back up your data to Acronis Cloud, the first backup may take a considerable amount of time to complete. Further backup processes will likely be much faster, because only changes to files will be transferred over the Internet.

4.3 Backing up mobile devices

If you have an iOS or Android smartphone or tablet, you can use Acronis True Image to protect your mobile data such as photos, video files, contacts, and calendars. Refer to Acronis True Image for mobile devices (p. 109) for details.

Copyright © Acronis International GmbH, 2002-2016

Before you start a backup, choose where you want to store the backup: Acronis Cloud or local storage on your computer. You can change the destination later, but you cannot back up to both destinations simultaneously. To back up the data to Acronis Cloud, use the Acronis True Image mobile app. Refer to Backing up your mobile device (p. 110) for details.

To back up mobile data to local storage on your computer:

1. Make sure that:
   - Acronis True Image 2017 is installed on your computer.
   - The Acronis True Image mobile app is installed on your mobile device.
   - Your mobile device and your computer are connected to the same Wi-Fi network.
2. On your computer:
   1. Start Acronis True Image.
   2. On the sidebar, click **Devices**, and then click **Mobile device local backup**.

      A QR code will be displayed. Please do not close this window.
3. On your mobile device:
   1. Start Acronis True Image.
   2. Tap **Back up to PC**.
   3. Tap **I already have it**, or follow the on-screen instructions to install Acronis True Image on your computer.
   4. Tap **Scan QR code**, point your camera at the QR code on the computer screen, and then wait until the mobile device is connected to the computer.
   5. Allow Acronis True Image to access the data that you want to back up. When you select all the data items, the backup starts automatically. Otherwise, tap **Back up anyway**.

      When the backup is started, you can track the progress in any application - on the computer or mobile device, but the errors and warning messages are displayed in the mobile app only.
   6. [Optional] If you want data changes (for example, new photographs) to be backed up automatically, make sure the **Continuous backup** setting is turned on. If this setting is turned off, the new data is backed up only when you tap **Back up**. Refer to Mobile app settings (p. 112) for details.

You can close both Acronis True Image on your computer and the Acronis True Image mobile app. The backup will continue in the background mode.

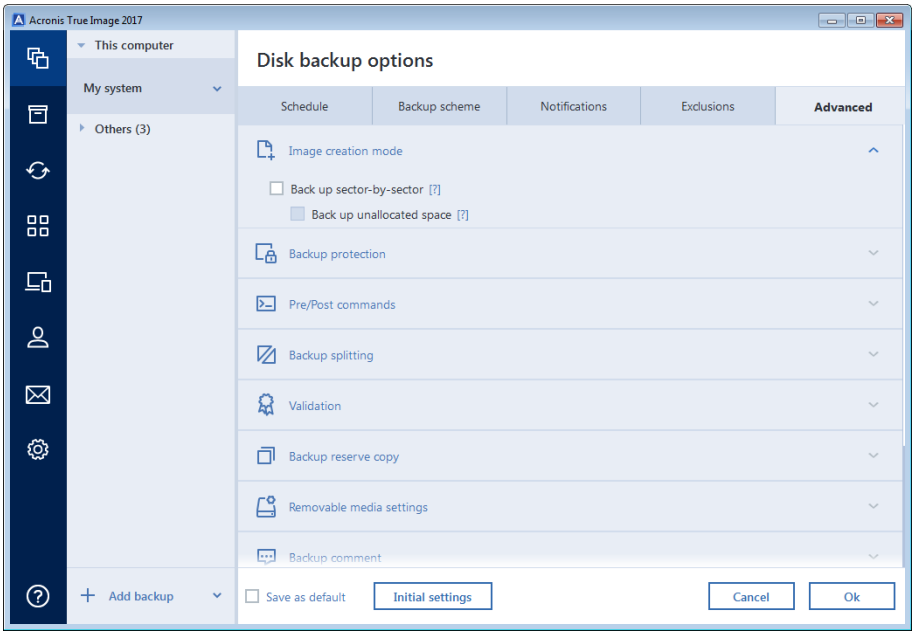
4.4 Backup options

When you create a backup, you can change additional options and fine-tune the backup process. To open the options window, select a source and destination for a backup, and then click **Options**.

Note that options of each backup type (disk-level backup, file-level backup, online backup, nonstop backup) are fully independent and you should configure them separately.

Copyright © Acronis International GmbH, 2002-2016

After you have installed the application, all options are set to the initial values. You can change them for your current backup operation only or for all backups that will be created in future. Select the **Save the settings as default** check box to apply the modified settings to all further backup operations by default.



If you want to reset all the modified options to the values that were set after the product installation initially, click the **Reset to initial settings** button. Note that this will reset the settings for the current backup only. To reset the settings for all further backups, click **Reset to initial settings**, select the **Save the settings as default** check box, and then click **OK**.

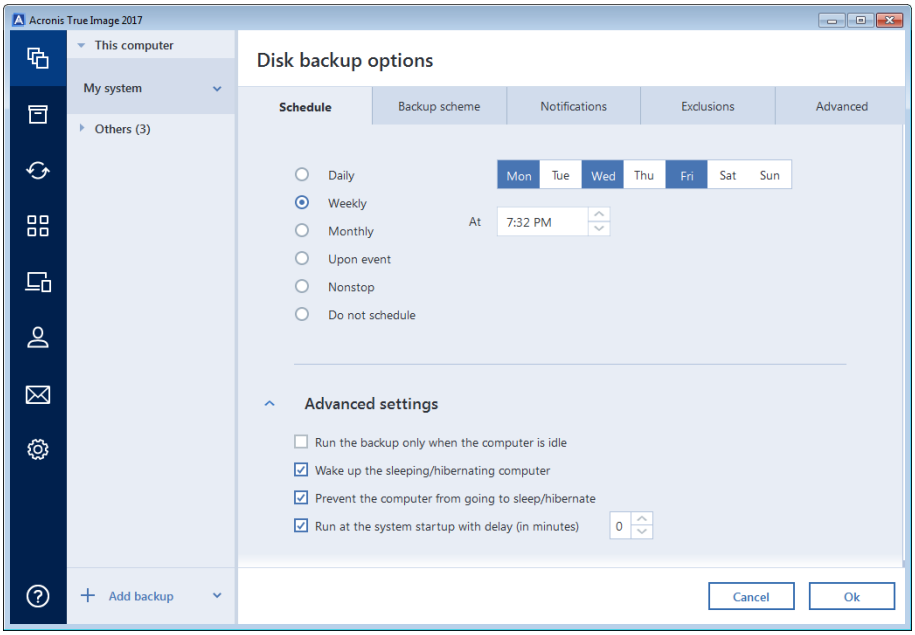
In this section

Scheduling 46
Backup schemes 48
Notifications for backup operation 53
Excluding items from backup 54
Image creation mode 56
Backup protection 56
Pre/Post commands for backup 57
Backup splitting 57
Backup validation option 58
Backup reserve copy 58
Removable media settings 59
Error handling 59
File-level security settings for backup 60
Computer shutdown 61
Acronis Cloud cleanup 61
Online backup protection 61
Selecting a data center for backup 62
Performance of backup operation 62

Copyright © Acronis International GmbH, 2002-2016

4.4.1 Scheduling

The **Schedule** tab allows you to specify the backup and validation schedule settings.



You can choose and set up one of the following backup or validation frequencies:

- **Nonstop** (p. 35)—The backup will run every five minutes.
- **Daily** (p. 47)—The operation will be executed once a day or more frequently.
- **Weekly** (p. 47)—The operation will be executed once a week or several times a week on the selected days.
- **Monthly** (p. 47)—The operation will be executed once a month or several times a month on the selected dates.
- **Upon event** (p. 47)—The operation will be executed upon an event.
- **Do not schedule**—The scheduler will be turned off for the current operation. In this case the backup or validation will run only when you click **Back up now** or **Validate** respectively in the main window.

Advanced settings

Clicking **Advanced settings** allows you to specify the following additional settings for backup and validation:

- To postpone a scheduled operation until the next time the computer is not in use (a screen saver is displayed or computer is locked), select the **Run the backup only when the computer is idle** check box. If you schedule validation, the check box will change to **Run the validation only when the computer is idle**.
- If you want to wake up the sleeping/hibernating computer to perform the scheduled operation, select the **Wake up the sleeping/hibernating computer** check box.
- When a backup takes a long time, it may be interrupted if the computer goes into sleep or hibernation mode. To eliminate this situation, select the **Prevent the computer from going to sleep/hibernate** check box.
- If the computer is switched off when the scheduled time comes, the operation won't be performed. You can force the missed operation to run at the next system startup. To do so, select the **Run at the system startup with delay (in minutes)** check box.

Copyright © Acronis International GmbH, 2002-2016

Additionally, you can set a time delay to start backup after the system startup. For example, to start backup 20 minutes after system startup, type *20* in the appropriate box.

- If you schedule a backup to a USB flash drive or validation of a backup that is located on a USB flash drive, one more check box appears: **Run when the current device is attached**. Selecting the check box will let you perform a missed operation when the USB flash drive is attached if it was disconnected at the scheduled time.

4.4.1.1 Daily execution parameters

You can set up the following parameters for daily operation execution:

- **Start time or periodicity**
  - If you select **At**, set the operation's start time. Enter hours and minutes manually, or set the desired start time using the up and down buttons. You can specify several start times by clicking **Add**.
  - If you select **Every**, choose daily operation periodicity from the dropdown list (for example, every 2 hours).

Description of the **Advanced settings** see in Scheduling (p. 46).

4.4.1.2 Weekly execution parameters

You can set up the following parameters for weekly operation execution:

- **Week days**

  Select the days on which to execute the operation by clicking on their names.
- **Start time**

  Set the operation's start time. Enter hours and minutes manually, or set the desired start time using the up and down buttons.

Description of the **Advanced settings** see in Scheduling (p. 46).

4.4.1.3 Monthly execution parameters

You can set up the following parameters for monthly operation execution:

- **Periodicity or dates**
  - If you select **Every**, choose a numeral and the day of the week from the dropdown lists (example: First Monday - the operation will be performed on the first Monday of every month)
  - If you select **On**, choose the date(s) for operation execution (example: you may want the operation to be run on the 10th, 20th, and last day of the month)
- **Start time**

  Set the operation's start time. Enter hours and minutes manually, or set the desired start time using the up and down buttons.

Description of the **Advanced settings** see in Scheduling (p. 46).

4.4.1.4 Upon event execution parameters

You can set up the following parameters for the Upon event operation execution:

- **Event**

Copyright © Acronis International GmbH, 2002-2016

- **User logon** – the operation will be executed each time the current user logs on to the OS.
- **User logoff** – the operation will be executed each time the current user logs off the OS.
- **System startup** – the operation will be executed at every OS startup.
- **System shutdown or restart** – the operation will be executed at every computer shutdown or reboot.

- **Additional condition**
  - If you want to run an operation only at the first occurrence of the event on the current day, select the **Once a day only** check box.

Description of the **Advanced settings** see in Scheduling (p. 46).

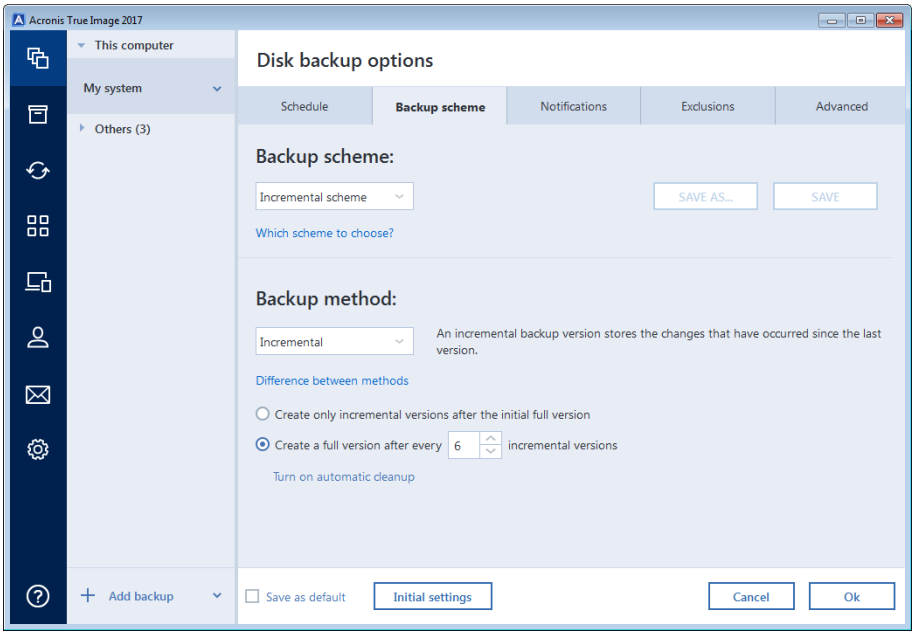
4.4.2 Backup schemes

Backup schemes along with the scheduler help you to set up your backup strategy. The schemes allow you to optimize backup storage space usage, improve data storage reliability, and automatically delete the obsolete backup versions.

For online backups, the backup scheme is preset and cannot be changed. After the initial full backup, only incremental versions are created.

The backup scheme defines the following parameters:

- Backup methods that will be used to create backup versions (full, differential or incremental)
- Sequence of the backup versions created using different methods
- Version cleanup rules



Acronis True Image allows you to choose from the following backup schemes:

- **Single version** (p. 49) - select this scheme if you want to use the smallest backup storage.
- **Version chain** (p. 49) - this may be the optimal scheme in many cases.
- **Incremental** - select to create a full version after every five incremental versions. This is the default scheme.
- **Differential** - select to create only differential backups after an initial full backup.

Copyright © Acronis International GmbH, 2002-2016

- **Custom** (p. 50) - select to set up a backup scheme manually.

You can easily change the backup scheme for a pre-existing backup. This will not affect the integrity of the backup chains, so you will be able to recover your data from any previous backup version.

You cannot change the backup scheme when backing up to optical media such as a DVD/BD. In this case, Acronis True Image by default uses a custom scheme with only full backups. This is because the program cannot consolidate backups stored on optical media.

4.4.2.1 Single version scheme

This backup scheme is the same for both disk backup and file backup types (except scheduler settings).

The program creates a full backup version and overwrites it every time according to the specified schedule or when you run the backup manually. In this process, the old version is deleted only after a new version is created.

Backup scheduler setting for disk backup: monthly.

Backup scheduler setting for file backup: daily.

Result: you have a single up-to-date full backup version.

Required storage space: minimal.

4.4.2.2 Version chain scheme

This backup scheme differs for disk backup and file backup types.

Disk backup version chain

At first the program creates the 1st full backup version. The version will be kept until you delete it manually. After that, according to the specified schedule (or when you run backup manually) the program creates: 1 full and 5 differential backup versions, then again 1 full and 5 differential backup versions and so on. The versions will be stored for 6 months. After the period the program analyzes if the oldest backup versions (except the 1st full version) may be deleted. It depends on the minimum number of versions (eight) and version chains consistency. The program deletes the oldest versions one by one after creating new versions with the same backup method (for example, the oldest differential version will be deleted after creation of the newest differential version). First of all the oldest differential versions will be deleted, then - the oldest full version.

Backup scheduler setting: monthly.

Result: you have monthly backup versions for the last 6 months plus the initial full backup version that may be kept for a longer period.

Required storage space: depends on the number of versions and their sizes.

File backup version chain

According to the specified schedule (or when you run backup manually) the program creates: 1 full and 6 incremental backup versions, then again 1 full and 6 incremental versions and so on. The versions will be stored for 1 month. After the period the program analyzes if the oldest backup versions may be deleted. It depends on the version chain consistency. To keep the consistency, the program deletes the oldest versions by chains "1 full + 6 incremental backup versions" after creating a new analogous version chain.

Copyright © Acronis International GmbH, 2002-2016

Backup scheduler setting: daily.

Result: you have backup versions for every day of the last month.

Required storage space: depends on the number of versions and their sizes.

4.4.2.3 Custom schemes

With Acronis True Image you also can create your own backup schemes. Schemes can be based on the pre-defined backup schemes. You can make changes in a selected pre-defined scheme to suit your needs and then save the changed scheme as a new one.

You cannot overwrite existing pre-defined backup schemes.

In addition, you can create custom schemes from scratch based on full, differential or incremental backup versions.

So first of all select one of the backup methods in the appropriate box.

- Full (p. 29)

  Select this method if you want to create only full backup versions.
- Differential (p. 29)

  Select this method if you want to create backup chains containing only full and differential backup versions.

  You can configure the scheme by using one of the following options:
  - **Create only differential versions after the initial full version** - select this item to create only one backup version chain. Automatic cleanup is not available for this option.
  - **Create a full version after every [n] differential versions** - select this item to create several backup version chains. This is a more reliable but more space-consuming backup scheme.
- Incremental (p. 29)

  Select this method if you want to create backup chains containing only full and incremental backup versions.

  You can configure the scheme by using one of the following options:
  - **Create only incremental versions after the initial full version** - select this item to create only one backup version chain. Automatic cleanup is not available for this option.
  - **Create a full version after every [n] incremental versions** - select this item to create several backup version chains. This is a more reliable but more space-consuming backup scheme.

Automatic cleanup rules

To delete obsolete backup versions automatically, you can set one of the following cleanup rules:

- **Delete versions older than [defined period]** (available for full method only) - Select this option to limit the age of backup versions. All versions that are older than the specified period will be automatically deleted.
- **Delete version chains older than [defined period]** (available for incremental and differential methods only) - Select this option to limit the age of backup version chains. The oldest version chain will be deleted only when the most recent backup version of this chain is older than the specified period.
- **Store no more than [n] recent versions** (available for full method only) - Select this option to limit the maximum number of backup versions. When the number of versions exceeds the specified value, the oldest backup version will be automatically deleted.

Copyright © Acronis International GmbH, 2002-2016

- **Store no more than [n] recent version chains** (available for incremental and differential methods only) - Select this option to limit the maximum number of backup version chains. When the number of version chains exceeds the specified value, the oldest backup version chain will be automatically deleted.
- **Keep size of the backup no more than [defined size]** - Select this option to limit maximum size of the backup. After creating a new backup version, the program checks whether the total backup size exceeds the specified value. If it's true, the oldest backup version will be deleted.

The first backup version option

Often the first version of any backup is one of the most valuable versions. This is true because it stores the initial data state (for example, your system partition with recently installed Windows) or some other stable data state (for example, data after a successful virus check).

Do not delete the first version of the backup - Select this check box to keep the initial data state. The program will create two initial full backup versions. The first version will be excluded from the automatic cleanup, and will be stored until you delete it manually.

If you select incremental or differential method, the first backup chain will start from the second full backup version. And only the third version of the backup will be incremental or differential one.

Note that when the check box is selected, the **Store no more than [n] recent versions** check box will change to **Store no more than 1+[n] recent versions**.

Managing custom backup schemes

If you change anything in an existing backup scheme, you can save the changed scheme as a new one. In this case you need to specify a new name for that backup scheme.

- You can overwrite existing custom schemes.
- You cannot overwrite existing pre-defined backup schemes.
- In a scheme name, you can use any symbols allowed by OS for naming files. The maximum length of a backup scheme name is 255 symbols.
- You can create not more than 16 custom backup schemes.

After creating a custom backup scheme, you can use it as any other existing backup scheme while configuring a backup.

You can also use a custom backup scheme without saving it. In this case, it will be available only for the backup where it was created and you will be unable to use it for other backups.

If you do not need a custom backup scheme anymore, you can delete it. To delete the scheme, select it in the backup schemes list, click **Delete**, and then click **Delete scheme** in the confirmation window.

The pre-defined backup schemes cannot be deleted.

Examples of custom schemes

1. Entire PC backup “Two full versions”

Case: You want to protect all data on your computer with two full versions and you want to update the backup once a month. Let’s see how you can do it by using a custom backup scheme.

1. Start configuring an entire PC backup. Refer to Backing up all data on your PC (p. 18) for details.
2. Make sure Entire PC is selected as the backup source.

Copyright © Acronis International GmbH, 2002-2016

3. Click **Options**, open the **Schedule** tab, click **Monthly**, and then specify a day of the month (for example, the 20-th). This will result in a backup version being created on a monthly basis, on the day you specify. Then, specify a start time for the backup operation.
4. Open the **Backup scheme** tab, and then choose **Custom scheme** instead of **Incremental scheme**.
5. In the **Backup method** box, select **Full** from the drop-down list.
6. To limit the number of versions, click **Store no more than [n] recent versions**, and type or select "2", and click **OK**.

   In this case, the program will create a new full version every month, on the 20-th day. After creating the third version, the oldest version will be automatically deleted.
7. Check that all settings are correct and click **Back up now**. If you want your first backup to be run only at the time you specified in the Scheduler, click the down arrow to the right of the **Back up now** button and select **Later** in the drop-down list.

2. File backup "Daily incremental version + weekly full version"

Case: You have files and/or folders you work with every day. You need to save your daily work results and want to be able to recover data state to any date for the last three weeks. Let's see how you can do this using a custom backup scheme.

1. Start configuring a file backup. Refer to Backing up files and folders for details.
2. Click **Options**, open the **Schedule** tab, click **Daily**, and then specify a start time for the backup operation. For example, if you finish your everyday work at 8 PM, specify this time or a little later (8.05 PM) as the start time.
3. Open the **Backup scheme** tab, and then choose **Custom scheme** instead of **Incremental scheme**.
4. In the **Backup method** box, select **Incremental** from the drop-down list.
5. Click **Create a full version after every [n] incremental versions**, and type or select "6".

   In that case, the program will first create the initial full backup version (no matter how you set up a backup process, the first backup version will always be the full one), and then six incremental versions day by day. Then, it will create one full version and six incremental versions again and so on. So every new full version will be created in exactly a week's time.
6. To limit the storage time for the versions, click **Turn on automatic cleanup**.
7. Click **Delete version chains older than [n] days**, type or select "21", and click **OK**.
8. Check that all settings are correct and click **Back up now**. If you want your first backup to run only at the time you specified in the Scheduler, click the down arrow to the right of the **Back up now** button and select **Later** in the drop-down list.

3. Disk backup "Full version every 2 months + differential version twice a month"

Case: You need to back up your system partition twice a month and create a new full backup version every two months. In addition, you want to use no more than 100 GB of disk space to store the backup versions. Let's see how you can do it using a custom backup scheme.

1. Start configuring a disk backup. Refer to Backing up disks and partitions (p. 41).
2. Select your system partition (usually C:) as the backup source.
3. Click **Options**, open the **Schedule** tab, click **Monthly**, and then specify, for example, the 1st and 15th days of the month. This will result in a backup version in about every two weeks. Then, specify a start time for the backup operation.
4. Open the **Backup scheme** tab, and then choose **Custom scheme** instead of **Incremental scheme**.
5. In the **Backup method** box, select **Differential** from the drop-down list.
6. Click **Create a full version after every [n] differential versions**, and type or select "3".

 Copyright © Acronis International GmbH, 2002-2016

In that case the program will first create the initial full backup version (no matter how you set up a backup process, the first backup version will always be the full one), and then three differential versions, each one in about two weeks. Then again a full version and three differential versions and so on. So every new full version will be created in two months.

7. To limit storage space for the versions, click **Turn on automatic cleanup**.
8. Click **Keep size of the backup no more than [defined size]**, type or select "100" "GB", and click **OK**.

   When the total backup size exceeds 100 GB, Acronis True Image will clean up the existing backup versions to make the remaining versions satisfy the size limit. The program will delete the oldest backup chain consisting of a full backup version and three differential backup versions.

9. Check that all settings are correct and click **Back up now**. If you want your first backup to be run only at the time you specified in the Scheduler, click the down arrow to the right of the **Back up now** button and select **Later** in the drop-down list.

4.4.3 Notifications for backup operation

Sometimes a backup or recovery procedure can last an hour or longer. Acronis True Image can notify you when it is finished via email. The program can also duplicate messages issued during the operation or send you the full operation log after operation completion.

By default, all notifications are disabled.

Free disk space threshold

You may want to be notified when the free space on the backup storage becomes less than the specified threshold value. If after starting a backup Acronis True Image finds out that the free space in the selected backup location is already less than the specified value, the program will not begin the actual backup process and will immediately inform you by displaying an appropriate message. The message offers you three choices - to ignore it and proceed with the backup, to browse for another location for the backup or to cancel the backup.

If the free space becomes less than the specified value while the backup is being run, the program will display the same message and you will have to make the same decisions.

To set the free disk space threshold:

- Select the **Show notification message on insufficient free disk space** check box
- In the **Size** box, type or select a threshold value and select a unit of measure

Acronis True Image can monitor free space on the following storage devices:

- Local hard drives
- USB cards and drives
- Network shares (SMB/NFS)

*The message will not be displayed if the **Do not show messages and dialogs while processing (silent mode)** check box is selected in the **Error handling** settings.*

This option cannot be enabled for FTP servers and CD/DVD drives.

Email notification

You can specify an email account that will be used to send you email notifications.

To configure the email notifications:

Copyright © Acronis International GmbH, 2002-2016

1. Select the **Send e-mail notifications about the operation state** check box.
2. Configure email settings:
   - Enter the email address in the **To** field. You can enter several email addresses in a semicolon-delimited format.
   - Enter the outgoing mail server (SMTP) in the **Outgoing mail server (SMTP)** field.
   - Set the port of the outgoing mail server. By default the port is set to 25.
   - If required, select the **SMTP authentication** check box, and then enter the user name and password in the corresponding fields.
3. To check whether your settings are correct, click the **Send test message** button.

If the test message sending fails, then perform the following:

1. Click **Show extended settings**.
2. Configure additional email settings:
   - Enter the e-mail sender address in the **From** field. If you are not sure what address to specify, then type any address you like in a standard format, for example *aaa@bbb.com*.
   - Change the message subject in the **Subject** field, if necessary.

     To simplify monitoring a backup status, you can add the most important information to the subject of the email messages. You can type the following text labels:
     - %BACKUP_NAME%—the backup name
     - %COMPUTER_NAME%—name of the computer where the backup was started
     - %OPERATION_STATUS%—result of the backup or other operation

       For example, you can type: *Status of backup %BACKUP_NAME%: %OPERATION_STATUS% (%COMPUTER_NAME%)*
   - Select the **Log on to incoming mail server** check box.
   - Enter the incoming mail server (POP3) in the **POP3 server** field.
   - Set the port of the incoming mail server. By default, the port is set to 110.
3. Click the **Send test message** button again.

Additional notification settings:

- To send a notification concerning process completion, select the **Send notification upon operation's successful completion** check box.
- To send a notification concerning process failure, select the **Send notification upon operation failure** check box.
- To send a notification with operation messages, select the **Send notification when user interaction is required** check box.
- To send a notification with full log of operations, select the **Add full log to the notification** check box.

4.4.4 Excluding items from backup

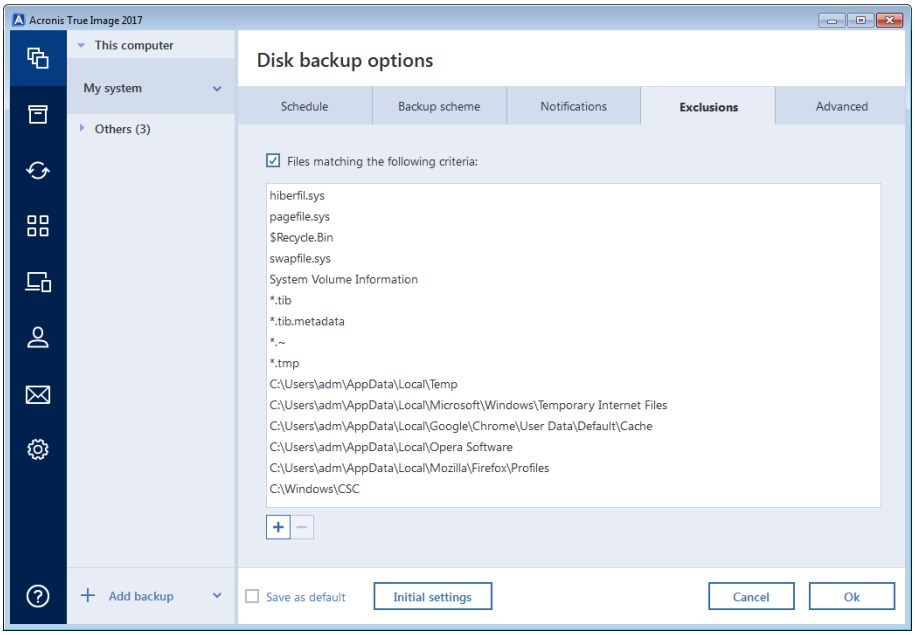
If you want to exclude unnecessary files from a backup, specify the appropriate file types on the **Exclusions** tab of the backup options. You can specify exclusions for disk backups, file backups or online backups.

When you select a specific file for backup, it cannot be excluded by the exclusion settings. The settings are applicable only to files located on a partition, disk, or inside a folder selected for backup.

Copyright © Acronis International GmbH, 2002-2016

How to use the default exclusion settings

After you have installed the application, all the exclusion settings are set to the initial values. You can change them for your current backup operation only or for all backups that will be created in future. Select the **Save as default** check box to apply the modified settings to all further backup operations by default. If you want to reset all the modified settings to the values that they were originally set to when the product was installed, click the **Reset to initial settings** button.



What you can exclude and how

You can exclude files meeting the criteria you specify. To do this, select the Files matching the following criteria check box, click the plus sign, and then enter the exclusion criterion.

We do not recommend excluding hidden and system files from the backups of your system partition.

How to add an exclusion criterion:

- You can enter explicit file names for exclusion from the backup:
  - *file.ext* - all such files will be excluded from the backup.
  - *C:\file.ext* - the file.ext file on the C: disk will be excluded.
- You can use wildcard characters (* and ?):
  - **.ext* - all files with a .ext extension will be excluded.
  - *??name.ext* - all files with a .ext extension, having six letters in their names (starting with any two symbols (??) and ending with *name*), will be excluded.
- To exclude a folder from a disk-level backup, click the plus sign, click the ellipsis button, go to the directory tree and select the folder you want to exclude, and then click **OK**.

To delete a criterion, for example, added by mistake, click the Delete icon to the right of the criterion.

4.4.4.1 Excluding online data

Before you start a backup, you can reduce the backup size by excluding data that does not need to be backed up. Acronis True Image now allows you to exclude your local data that is uploaded or

Copyright © Acronis International GmbH, 2002-2016

synchronized with third-party Cloud services, such as Dropbox or Microsoft OneDrive. This data is already reliably protected and can be easily downloaded to your computer. Therefore you can exclude it to reduce the backup size and to speed up the backup process.

To exclude an online data source from a backup:

1. Before you start the backup process, click **Exclude items from backup**.
2. Clear the check boxes next to the items that you want to exclude, and then click **OK**.

4.4.5 Image creation mode

You can use these parameters to create an exact copy of your whole partitions or hard disks, and not only the sectors that contain data. For example, this can be useful when you want to back up a partition or disk containing an operating system that is not supported by Acronis True Image. Please note that this mode increases processing time and usually results in a larger image file.

- To create a sector-by-sector image, select the **Back up sector-by-sector** check box.
- To include all unallocated disk space into the backup, select the **Back up unallocated space** check box.

  This check box is available only when the **Back up sector-by-sector** check box is selected.

4.4.6 Backup protection

A backup file can be password-protected. By default, there is no password protection for backups.

You cannot set or change the backup protection option for a pre-existing backup.

To protect a backup:

1. Enter the password for the backup into the corresponding field. We recommend that you use a password longer than seven symbols and containing both letters (in upper and lower cases preferably) and numbers to make it more difficult to guess.

   A password cannot be retrieved. Please memorize the password that you specify for a backup protection.
2. To confirm the previously entered password, retype it into the corresponding field.
3. [optional step] To increase the security of your confidential data, you can encrypt the backup with strong industry-standard AES (Advanced Encryption Standard) cryptographic algorithm. AES is available with three key lengths – 128, 192 and 256 bits to balance performance and protection as desired.

   The 128-bit encryption key is sufficient for most applications. The longer the key, the more secure your data. However, the 192 and 256-bit long keys significantly slow down the backup process.

   If you want to use AES encryption, choose one of the following keys:

   - **AES 128** - to use 128-bit encryption key
   - **AES 192** - to use 192-bit encryption key
   - **AES 256** - to use 256-bit encryption key

   If you do not want to encrypt the backup and only want to protect a backup with a password, select **None**.
4. Having specified the backup settings, click **OK**.

Copyright © Acronis International GmbH, 2002-2016

How to get access to a password-protected backup

Acronis True Image asks for the password every time you try to modify the backup:

- Recover data from the backup
- Edit settings
- Delete
- Mount
- Move

To access the backup, you must specify the correct password.

4.4.7 Pre/Post commands for backup

You can specify commands (or even batch files) that will be automatically executed before and after the backup procedure.

For example, you may want to start/stop certain Windows processes, or check your data before starting backup.

To specify commands (batch files):

- Select a command to be executed before the backup process starts in the **Pre-command** field. To create a new command or select a new batch file, click the **Edit** button.
- Select a command to be executed after the backup process ends in the **Post-command** field. To create a new command or select a new batch file, click the **Edit** button.

Please do not try to execute interactive commands, i.e. commands that require user input (for example, "pause"). These are not supported.

4.4.7.1 Edit user command for backup

You can specify user commands to be executed before or after the backup procedure:

- In the **Command** field, type-in a command or select it from the list. Click **...** to select a batch file.
- In the **Working directory** field, type-in a path for command execution or select it from the list of previously entered paths.
- In the **Arguments** field enter or select command execution arguments from the list.

Disabling the **Do not perform operations until the command's execution is complete** parameter (enabled for Pre commands by default), will permit the backup process to run concurrently with your command execution.

The **Abort the operation if the user command fails** (enabled by default) parameter will abort the operation if any errors occur in command execution.

You can test a command you entered by clicking the **Test command** button.

4.4.8 Backup splitting

Acronis True Image cannot split already existing backups. Backups can be split only when being created.

Large backups can be split into several files that together make up the original backup. A backup can also be split for burning to removable media.

Copyright © Acronis International GmbH, 2002-2016

The default setting - **Automatic**. With this setting, Acronis True Image will act as follows.

When backing up to a hard disk:

- If the selected disk has enough space and its file system allows the estimated file size, the program will create a single backup file.
- If the storage disk has enough space, but its file system does not allow the estimated file size, the program will automatically split the image into several files.
- If you do not have enough space to store the image on your hard disk, the program will warn you and wait for your decision as to how you plan to fix the problem. You can try to free some additional space and continue or select another disk.

When backing up to a CD-R/RW, DVD-R/RW, DVD+R/RW, BD-R/RE:

- Acronis True Image will ask you to insert a new disk when the previous one is full.

Alternatively, you may select the desired file size from the drop-down list. The backup will then be split into multiple files of the specified size. This is useful when you store a backup to a hard disk in order to burn the backup to CD-R/RW, DVD-R/RW, DVD+R/RW or BD-R/RE later on.

Creating images directly on CD-R/RW, DVD-R/RW, DVD+R/RW, BD-R/RE might take considerably more time than it would on a hard disk.

4.4.9 Backup validation option

You can specify the following settings:

- **Validate backup when it is created** - Select to check the integrity of the backup version immediately after backup. We recommend that you enable this option when you back up your critical data or system disk.
- **Validate backup regularly** - Select to schedule validation of your backups to ensure that they remain "healthy".

  The default settings are as follows:

  - **Frequency:** once a month.
  - **Day:** the date when the backup was started.
  - **Time:** the moment of backup start plus 15 minutes.
  - **Advanced settings:** the **Run the validation only when the computer is idle** check box is selected.

  Example: You start a backup operation on July 15, at 12.00. The backup version is created at 12.05. Its validation will run at 12.15 if your computer is in the "screen saver" state at the moment. If not, then the validation will not run. In a month, August 15, at 12.15, the validation will start again. As before, your computer must be in the "screen saver" state. The same will occur on September 15, and so on.

  You can change the default settings and specify your own schedule. For more information see Scheduling (p. 46).

4.4.10 Backup reserve copy

Backup reserve copy is an independent full backup version created immediately after a normal backup. Even when you create an incremental or differential backup version containing only data changes, the reserve copy will contain all the data selected for the normal backup. You can save reserve copies of your backups on the file system, a network drive, or a USB flash drive.

 Copyright © Acronis International GmbH, 2002-2016

Please, be aware that CD/DVDs are not supported as locations for reserve copies.

To make a reserve copy:

1. Select the **Create a reserve copy of my backups** check box.
2. Specify a location for the backup copies.

   You can protect the reserve copy with a password. All other backup options will be inherited from the source backup.

4.4.11 Removable media settings

When backing up to removable media, you can make this media bootable by writing additional components to it. Thus, you will not need a separate bootable disk.

Acronis True Image does not support creating bootable media if a flash drive is formatted in NTFS or exFAT. The drive must have a FAT16 or FAT32 file system.

The following settings are available:

- **Place Acronis True Image on media**

  Acronis True Image - includes support of USB, PC Card (formerly PCMCIA) and SCSI interfaces along with the storage devices connected via them, and therefore is strongly recommended.
- **Place Acronis System Report on media**

  Acronis System Report - the component allows you to generate system report that is used for collecting information about your system in case of any program problem. Report generation will be available before you start Acronis True Image from the bootable media. The generated system report can be saved to a USB flash drive.
- **Place Acronis One-Click Restore on media**

  Acronis One-Click Restore is a minimal addition to your bootable media, allowing one-click data recovery from an image backup stored on this media. This means that when booting from the media and after clicking **Recover**, all data will be silently recovered to its original place. No options or selections such as resizing partitions will be possible.

  Acronis One-Click Restore can be added to the media only when creating a full backup of an entire hard disk.
- **Ask for first media while creating backups on removable media**

  You can choose whether to display the Insert First Media prompt when backing up to removable media. With the default setting, backing up to removable media may not be possible if the user is away, because the program will wait for someone to press OK in the prompt box. Therefore, you should disable the prompt when scheduling a backup to removable media. Then, if the removable media is available (for example, CD-R/RW inserted) the backup can run unattended.

If you have other Acronis products installed on your computer, the bootable versions of these programs' components will be offered as well.

4.4.12 Error handling

When the program encountered an error while performing backup, it stops the backup process and displays a message, waiting for a response on how to handle the error. If you set an error handling policy, the program will not stop the backup process, but will simply handle the error according to the set rules and continue working.

Copyright © Acronis International GmbH, 2002-2016

You can set the following error handling policy:

- **Do not show messages and dialogs while processing (silent mode)** - Enable this setting to ignore errors during backup operations. This is useful when you cannot control the backup process.
- **Ignore bad sectors** - This option is available only for disk and partition backups. It lets you successfully complete a backup even if there are bad sectors on the hard disk.

  We recommend that you select this check box when your hard drive is failing, for example:

  - Hard drive is making clicking or grinding noises during operation.
  - The S.M.A.R.T. system has detected hard drive issues and recommends that you back up the drive as soon as possible.

  When you leave this check box cleared, the backup may fail because of possible bad sectors on the drive.
- **When not enough space in ASZ, delete the oldest backup** (the preset is enabled) - We recommend that you select this check box when planning unattended scheduled backups to the Acronis Secure Zone. Otherwise, when the Acronis Secure Zone is full during a backup operation, Acronis True Image suspends the backup and requires your action. The dialog will open even when the **Do not show messages and dialogs while processing (silent mode)** setting is enabled.
- **Repeat attempt if a backup fails** - This option allows you to automatically repeat a backup attempt if the backup fails for some reason. You can specify number of attempts and time interval between attempts. Note that if the error interrupting the backup persists, then the backup will not be created.

  This option is not available, when you back up your data to a USB flash drive or USB hard drive.

4.4.13 File-level security settings for backup

You can specify security settings for backed up files (these settings relate only to file/folder backups):

- **Preserve file security settings in backups** - selecting this option will preserve all the security properties (permissions assigned to groups or users) of the backup files for further recovery.

  By default, files and folders are saved in the backup with their original Windows security settings (i.e. permissions for read, write, execute and so on for each user or user group, set in file **Properties** -> **Security**). If you recover a secured file/folder on a computer without the user specified in the permissions, you may not be able to read or modify this file.

  To eliminate this kind of problem, you can disable preserving file security settings in backups. Then the recovered files/folders will always inherit the permissions from the folder to which they are recovered (parent folder or disk, if recovered to the root).

  Or, you can disable file security settings during recovery, even if they are available in the backup. The result will be the same.
- **In backups, store encrypted files in a decrypted state** (the preset is disabled) - check the option if there are encrypted files in the backup and you want them to be accessed by any user after recovery. Otherwise, only the user who encrypted the files/folders will be able to read them. Decryption may also be useful if you are going to recover encrypted files on another computer.

  If you do not use the encryption feature available in Windows XP and later operating systems, simply ignore this option. (Files/folders encryption is set in **Properties** -> **General** -> **Advanced Attributes** -> **Encrypt contents to secure data**).

These options relate only to file/folder backups.

Copyright © Acronis International GmbH, 2002-2016

4.4.14 Computer shutdown

If you know that the backup process you are configuring may take a long time, you may select the **Shut down the computer after the backup is complete** check box. In this case, you will not have to wait until the operation completion. The program will perform the backup and turn off your computer automatically.

This option is also useful when you schedule your backups. For example, you may want to perform backups every weekday in the evening to save all your work. Schedule the backup and select the check box. After that you may leave your computer when you finish your work knowing that the critical data will be backed up and the computer will be turned off.

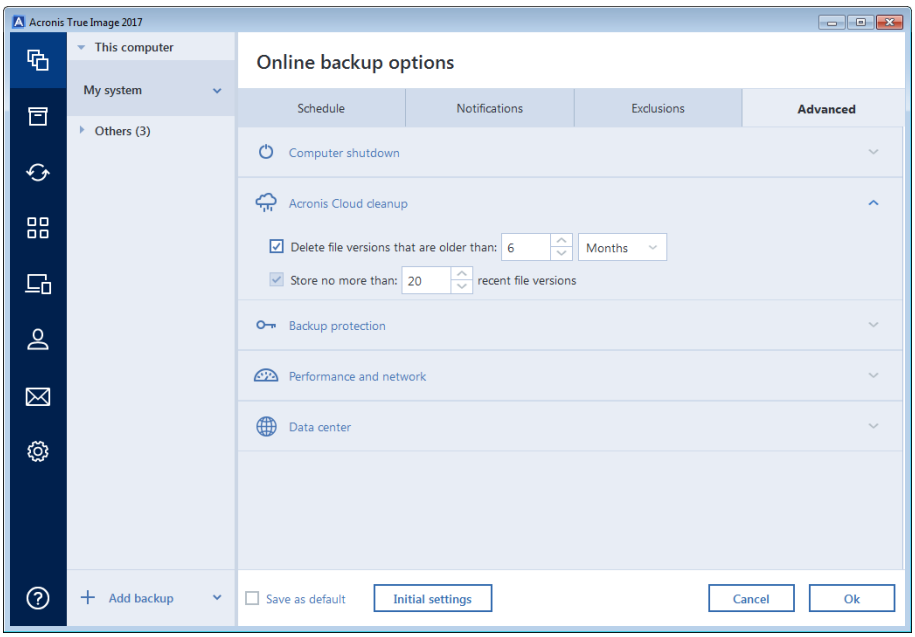
4.4.15 Acronis Cloud cleanup

This option is only available for online backup.

You can configure the cleanup settings for Acronis Cloud to optimize usage of its space.

To set the limits for the amount of versions on Acronis Cloud:

- Select the **Delete versions that are older than** check box and enter a value that limits the maximum age of the older versions. All other versions will be automatically deleted except the most recent versions.
- Select the **Store no more than … recent versions** check box and enter a value that limits the maximum number of all versions in the storage.



4.4.16 Online backup protection

To protect your data on Acronis Cloud from unauthorized access, you can use encryption. In this case, your data will be stored on Acronis Cloud in an encrypted form. To encrypt and decrypt your data, the program needs the password, that you should specify when you configure the online backup. You can specify any set of characters you like. Note that the password is case-sensitive.

⚠ Warning! A password of an online backup cannot be retrieved. Please memorize the password that you specify for backup protection.

Copyright © Acronis International GmbH, 2002-2016

While attempting to access the encrypted data, the program asks you to enter the password.

Note that you cannot set or change the password for a pre-existing online backup.

4.4.17 Selecting a data center for backup

This option is only available for online backup.

When you create a backup to Acronis Cloud, your data is uploaded to one of the Acronis data centers located in different countries. Initially, the data center is defined as the one closest to your location when you create your Acronis account. Afterwards, your online backups and synced files are stored in the same data center, by default.

We recommend that you set the data center for a backup manually, when you are in a different country and your default data center is not the closest to your current location. This will significantly increase the data upload rate.

Note: You cannot change the data center for a pre-existing backup.

To select a data center:

1. On the Online Backup Options screen, click **Advanced**, and then click **Data center**.
2. Select the country that is closest to your current location.

4.4.18 Performance of backup operation

Compression level

You can choose the compression level for a backup:

- **None** - the data will be copied without any compression, which may significantly increase the backup file size.
- **Normal** - the recommended data compression level (set by default).
- **High** - higher backup file compression level, takes more time to create a backup.
- **Maximum** - maximum backup compression, but takes a long time to create a backup.

The optimal data compression level depends on the type of files stored in the backup. For example, even maximum compression will not significantly reduce the backup size, if the backup contains essentially compressed files, like .jpg, .pdf or .mp3.

You cannot set or change the compression level for a pre-existing backup.

Operation priority

Changing the priority of a backup or recovery process can make it run faster or slower (depending on whether you raise or lower the priority), but it can also adversely affect the performance of other running programs. The priority of any process running in a system, determines the amount of CPU usage and system resources allocated to that process. Decreasing the operation priority will free more resources for other CPU tasks. Increasing backup or recovery priority may speed up the process by taking resources from the other currently running processes. The effect will depend on total CPU usage and other factors.

You can set up the operation priority:

Copyright © Acronis International GmbH, 2002-2016

- **Low** (enabled by default) - the backup or recovery process will run slower, but the performance of other programs will be increased.
- **Normal** - the backup or recovery process will have the equal priority with other processes.
- **High** - the backup or recovery process will run faster, but the performance of other programs will be reduced. Be aware that selecting this option may result in 100% CPU usage by Acronis True Image.

Network connection transfer rate

When you back up data to Acronis Cloud, network drives, or FTP, you can change the connection speed used by Acronis True Image. Set the connection speed that will allow you to use Internet and network resources without annoying slowdowns.

To set up the connection speed, select one of the following options:

- **Optimal**

  The data transfer rate is not changed by Acronis True Image.
- **Maximum** (available for online backups only)

  This option significantly speeds up the upload process, but at the same time the Internet connection speed decreases for other applications. The optimization mechanism splits the data into small portions, and then uploads these portions via multiple network connections. In the target Acronis data center, the split data is assembled back to the initial state, and then stored in the cloud storage.
- **Limit upload speed to**

  You can specify a maximum value for data upload speed.

4.5 Operations with backups

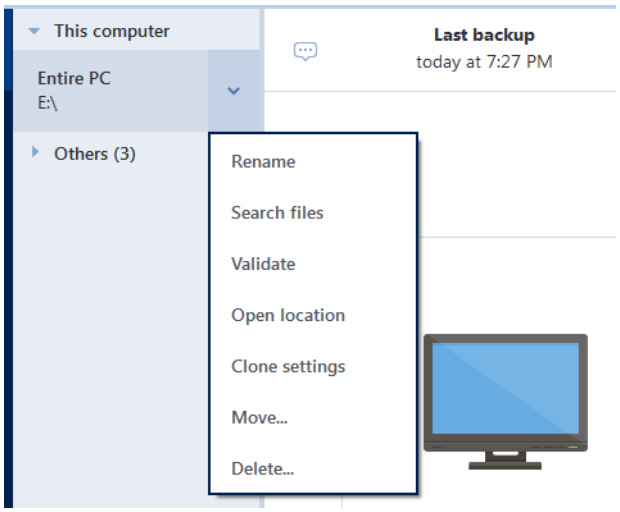
In this section

Backup operations menu 64
Sorting backups in the list 65
Validating backups 65
Backup to various places 66
Adding an existing backup to the list 66
Deleting backups and backup versions 66
Backing up to Acronis Cloud from several computers 68
Removing data from Acronis Cloud 68

Copyright © Acronis International GmbH, 2002-2016

4.5.1 Backup operations menu

The backup operations menu provides quick access to additional operations that can be performed with the selected backup.



The backup operations menu can contain the following items:

- **Rename** (not available for online backups) - allows you to set a new name for a backup in the list. The backup files will not be renamed.
- **Reconfigure** (for backups manually added to the backup list) - allows configuring the settings of a backup created by a previous Acronis True Image version. This item may also appear for backups created on another computer and added to the backup list without importing their settings.

  Without backup settings, you cannot refresh the backup by clicking **Back up now**. Also, you cannot edit and clone the backup settings.
- **Reconfigure** (for online backups) - allows you to bind a selected online backup to the current computer. To do this, click this item and reconfigure settings of the backup. Note that only one online backup can be active on one computer.
- **Validate** - starts backup validation.
- **Open location** - opens the folder containing the backup files.
- **Clone settings** - Creates a new empty backup box with the settings of the initial backup and named **(1) [the initial backup name]**. Change the settings, save them, and then click **Back up now** on the cloned backup box.
- **Move** - click to move all the backup files to another location. The subsequent backup versions will be saved to the new location.

  If you change the backup destination by editing the backup settings, only new backup versions will be saved to the new location. The earlier backup versions will remain in the old location.
- **Delete** - depending on a backup type, this command completely deletes the backup from its location or allows you to choose whether you want to delete the backup completely or the backup box only. When you delete a backup box, the backup files remain in the location, and you will be able to add the backup to the list later. Note that when you delete a backup completely, the deletion cannot be undone.

Copyright © Acronis International GmbH, 2002-2016

4.5.2 Sorting backups in the list

By default, the backups are sorted by the date they were created, starting from the newest to oldest. To change the order, select the appropriate sorting type in the upper part of the backup list. You have the following options:

Command		Description
Sort by	**Name**	This command sorts all backups in alphabetical order. To reverse the order, select **Z —> A**.
	Date created	This command sorts all backups from newest to oldest. To reverse the order, select **Oldest on top**.
	Date updated	This command sorts all backups by date of the last version. The newer the last backup version, the higher the backup will be placed in the list. To reverse the order, select **Least recent on top**.
	Size	This command sorts all backups by size, from biggest to smallest. To reverse the order, select **Smallest on top**.
	Source type	This command sorts all backups by the source type. The order is as follows: entire PC backups - disk backups - file backups - nonstop backup.
	Destination type	This command sorts all backups by the destination type. The order is as follows: internal disk drives - external disk drives - NAS devices - network shares - Acronis Cloud.

4.5.3 Validating backups

The validation procedure checks whether you will be able to recover data from a backup.

Validating backups in Windows

To validate an entire backup:

1. Start Acronis True Image, and then click **Backup** on the sidebar.
2. In the backup list, right-click the backup to validate, and then click **Validate**.

Validating backups in a stand-alone version of Acronis True Image (bootable media)

To validate a specific backup version or an entire backup:

1. On the **Recovery** tab, find the backup that contains the version that you want to validate. If the backup is not listed, click **Browse for backup**, and then specify the path to the backup. Acronis True Image adds this backup to the list.
2. Right-click the backup or a specific version, and then click **Validate Archive**. This opens the **Validate Wizard**.
3. Click **Proceed**.

Copyright © Acronis International GmbH, 2002-2016

4.5.4 Backup to various places

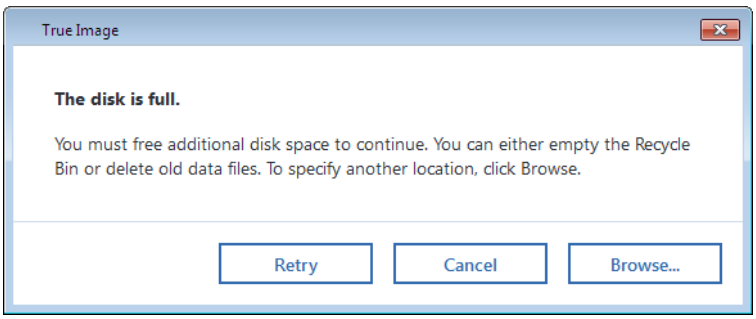
You can save versions of a backup to different destinations by changing the backup destination when editing the backup settings. For example, after you save the initial full backup to an external USB hard drive, you can change the backup destination to a USB stick by editing the backup settings. The subsequent incremental or differential backups will be written to the USB stick.

You cannot continue backing up to an optical disc.

Acronis Secure Zone and FTP servers can contain an entire backup only.

Splitting backups on-the-fly

When free space on the destination storage is insufficient to complete the current backup operation, the program displays a message warning you that the disk is full.


True Image
The disk is full.
You must free additional disk space to continue. You can either empty the Recycle Bin or delete old data files. To specify another location, click Browse.
Retry
Cancel
Browse...

To complete the backup, perform one of the following:

- Free up some space on the disk and click **Retry**.
- Click **Browse**, and then select another storage device.

When versions of a backup are stored in different locations, you may need to specify the locations during recovery.

4.5.5 Adding an existing backup to the list

You may have Acronis True Image backups created by a previous product version or copied from another computer. Every time you start Acronis True Image, it scans your computer for such backups and adds them to the backup list automatically.

If you have backups that are not shown in the list, you can add them manually.

To add backups manually:

1. In the **Backup** section, at the bottom of the backup list, click the arrow icon, and then click **Add existing backup**. The program opens a window where you can browse for backups on your computer.
2. Select a backup version (a .tib file), and then click **Add**.

   The entire backup will be added to the list.

4.5.6 Deleting backups and backup versions

This topic is applicable to local and network backups. For information about deleting online backups, refer to Removing data from Acronis Cloud (p. 68).

Copyright © Acronis International GmbH, 2002-2016

When you want to delete backups and backup versions you no longer need, please do it by using the tools provided by Acronis True Image.

Acronis True Image stores information on the backups in a metadata information database. Therefore, deleting unneeded backup files in File Explorer will not delete information about these backups from the database. This will result in errors when the program tries to perform operations on the backups that no longer exist.

To delete an entire backup:

In the **Backup** section, right-click a backup in the backup list, and then click **Delete**.

Depending on a backup type, this command completely deletes the backup from its location or allows you to choose whether you want to delete the backup completely or the backup box only. When you delete a backup box only, the backup files remain in the location, and you will be able to add the backup to the list later. Note that if you delete a backup completely, the deletion cannot be undone.

To configure automatic cleanup rules for a backup:

1. Go to the **Backup** section.
2. Perform one of the following:
   - For a new backup, click **Add backup**, choose **Create new backup**, select backup source and destination, and then click **Options**.
   - For an existing backup, select the backup from the backup list, click **Operations**, choose **Edit settings**, and then click **Options**.
3. On the **Backup scheme** tab, select **Custom scheme**, select a backup method, and then click **Turn on automatic cleanup**.
4. Configure cleanup rules for the backup. Refer to Custom schemes (p. 50) for details.

To delete a specific backup version:

1. Start your computer by using bootable media. Refer to Arranging boot order in BIOS (p. 81) for details.
2. In the Recovery section, click Refresh backups. This will update the backup list. If you cannot find the target backup in the list, or the backup is located on removable media, click Browse for backup, and provide the path to the backup.
3. Depending on type of the backup, go to the Disk backups or File backups tab.
4. Right-click the backup version that you want to delete, and then click Remove. The opened window displays the list of backup versions that will be deleted. See below why this list may contain more than one backup version.
5. To confirm the deletion, click Delete.

Why does Acronis True Image sometimes delete more than one backup version?

When you delete a backup version, please remember that this version may have dependent versions. In this case the dependent versions will be deleted as well, because data recovery from such versions becomes impossible.

- **If you delete a full backup version** - the program will also delete all subsequent incremental and differential versions till the next full version.
- **If you delete an incremental backup version or a differential backup version** - the program will also delete all subsequent incremental versions till the next full or differential version.

Copyright © Acronis International GmbH, 2002-2016

See also Full, incremental and differential backups (p. 29).

4.5.7 Backing up to Acronis Cloud from several computers

When you want to back up data to Acronis Cloud under the same Acronis account, we recommend that you create a separate online backup on each computer. This allows you to avoid mixture of data from different computers within one online backup.

However, you may want to switch between your computers and back up data to the same online backup. When you sign in to your Acronis account, Acronis True Image tries to find out whether you already have online backups created on other computers. If this is the case, the program adds them to the backup list. To activate any of these backups on the current computer, click **Operations**, click **Reconfigure**, select backup source, and then click **Save**. After that, you can back up data of the current computer to the selected backup, but this backup will be stopped on the other computer. The backed up data from the previous computer is not deleted and remains available for recovery.

4.5.8 Removing data from Acronis Cloud

Because the available space on Acronis Cloud is limited, you need to manage your Cloud space by cleaning up the obsolete data or the data you do not need anymore. Cleanup can be done in a variety of ways.

Deleting entire backup

The most "drastic" one is deleting the entire backup from a computer on Acronis Cloud. To remove the backup, click the gear icon on an online backup box and then click **Delete**.

Cleanup settings

The Online backup options provide for automatic cleanup of Acronis Cloud. You can specify deletion of files that have been kept longer than the specified number of months or days. In addition, you can set the maximum number of file versions to be kept on Acronis Cloud. You can accept the default settings for those options or set the values you need. For more information see Acronis Cloud cleanup (p. 61).

One-time cleanup

When your Acronis Cloud is full or is running out of space, we recommend that you use the cleanup tool in Acronis Cloud web application. This tool allows you to free up considerable amount of space on the cloud fast and easy.

To clean up Acronis Cloud:

1. Start Acronis True Image and click **Recover** on an online backup box. You will be taken to the Acronis Cloud web application.
2. On the **Storage status** tab, click the **Clean up space** link in the center of the screen.
3. In the opened window, configure the cleanup settings and click **Clean up now.**

Deleting specific files and folders

You can also manage Acronis Cloud by deleting individual files and folders.

1. Start Acronis True Image and click **Recover** on an online backup box. You will be taken to the Acronis Cloud web application.
2. Select files and folders you want to delete and click the **Delete** button.

Copyright © Acronis International GmbH, 2002-2016

5 Recovering data

In this section

Recovering disks and partitions 69
Recovering files and folders 82
Searching backup content 83
Recovery from Acronis Cloud 84
Recovery options 89

5.1 Recovering disks and partitions

In this section

Recovering your system after a crash 69
Recovering partitions and disks 78
About recovery of dynamic/GPT disks and volumes 79
Arranging boot order in BIOS 81

5.1.1 Recovering your system after a crash

When your computer fails to boot, it is advisable to at first try to find the cause using the suggestions given in Trying to determine the crash cause (p. 69). If the crash is caused by corruption of the operating system, use a backup to recover your system. Make the preparations described in Preparing for recovery (p. 70) and then proceed with recovering your system.

5.1.1.1 Trying to determine the crash cause

A system crash can be due to two basic factors:

- **Hardware failure**

  In this scenario, it is better to let your service center handle the repairs. However, you may want to perform some routine tests. Check the cables, connectors, power of external devices, etc. Then, restart the computer. If there is a hardware problem, the Power-On Self Test (POST) will inform you about the failure.

  If the POST does not reveal a hardware failure, enter BIOS and check whether it recognizes your system hard disk drive. To enter BIOS, press the required key combination (**Del**, **F1**, **Ctrl+Alt+Esc**, **Ctrl+Esc**, or some other, depending on your BIOS) during the POST sequence. Usually the message with the required key combination is displayed during the startup test. Pressing this combination takes you to the setup menu. Go to the hard disk autodetection utility which usually comes under "Standard CMOS Setup" or "Advanced CMOS setup". If the utility does not detect the system drive, it has failed and you need to replace the drive.

- **Operating system corruption (Windows cannot start up)**

  If the POST correctly detects your system hard disk drive, then the cause of the crash is probably a virus, malware or corruption of a system file required for booting. In this case, recover the system using a backup of your system disk or system partition. Refer to Recovering your system (p. 70) for details.

Copyright © Acronis International GmbH, 2002-2016

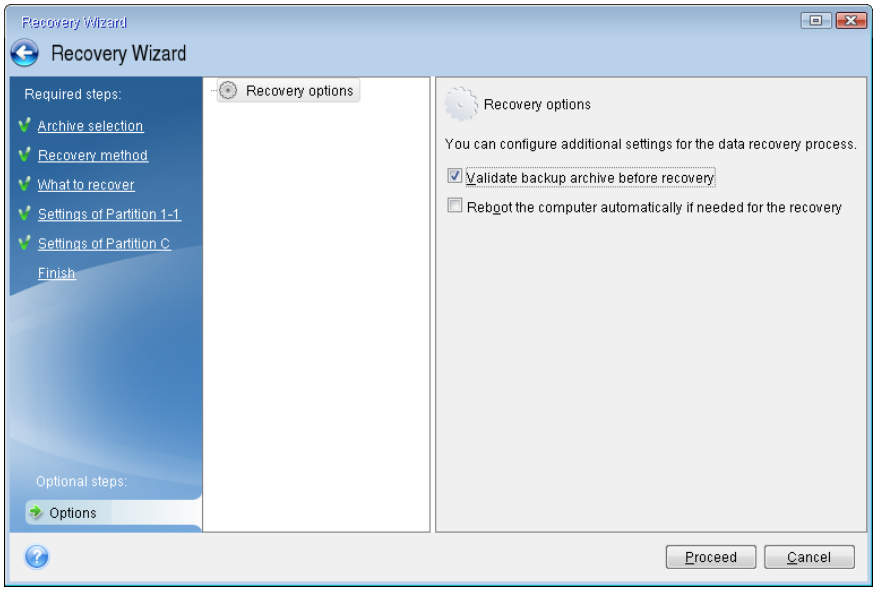
5.1.1.2 Preparing for recovery

We recommend that you perform the following actions before recovery:

- Scan the computer for viruses if you suspect that the crash occurred due to a virus or malware attack.
- Under bootable media, try a test recovery to a spare hard drive, if you have one.
- Validate the image under bootable media. A backup that can be read during validation in Windows, **may not always be readable in a Linux environment**.

  Under bootable media, there are two ways to validate a backup:

  - To validate a backup manually, on the **Recovery** tab, right-click a backup and select **Validate Archive**.
  - To validate a backup automatically before recovery, on the **Options** step of the **Recovery Wizard**, select the **Validate backup archive before recovery** check box.



- Assign unique names (labels) to all partitions on your hard drives. This will make finding the disk containing your backups easier.

  When you use the Acronis True Image rescue media, it creates disk drive letters that might differ from the way Windows identifies drives. For example, the D: disk identified in the standalone Acronis True Image might correspond to the E: disk in Windows.

5.1.1.3 Recovering your system to the same disk

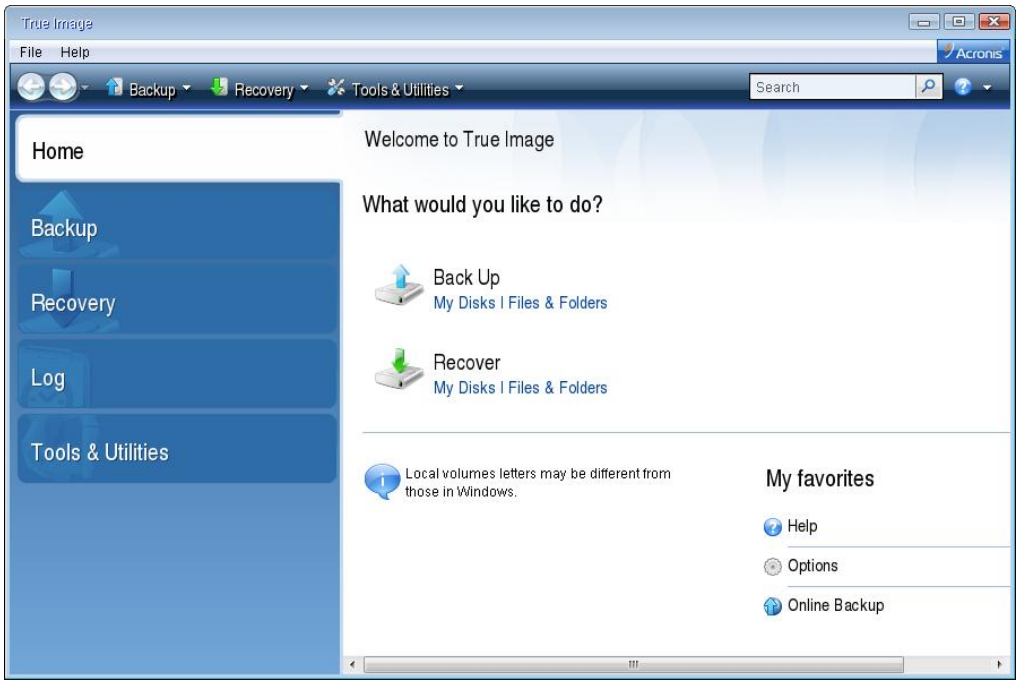
Before you start, we recommend that you complete the procedures described in Preparing for recovery (p. 70).

To recover your system:

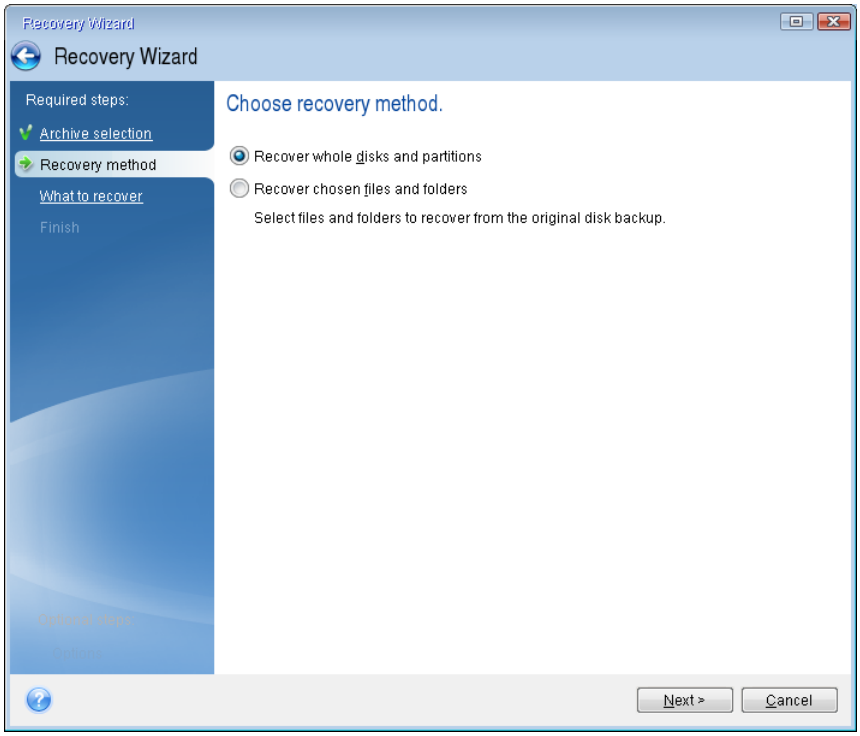
1. Attach the external drive if it contains the backup to be used for recovery and make sure that the drive is powered on.
2. Arrange the boot order in BIOS so as to make your rescue media device (CD, DVD or USB stick) the first boot device. See Arranging boot order in BIOS (p. 81).
3. Boot from the rescue media and select **Acronis True Image**.

Copyright © Acronis International GmbH, 2002-2016

4. On the **Home** screen, select **My disks** below **Recover**.

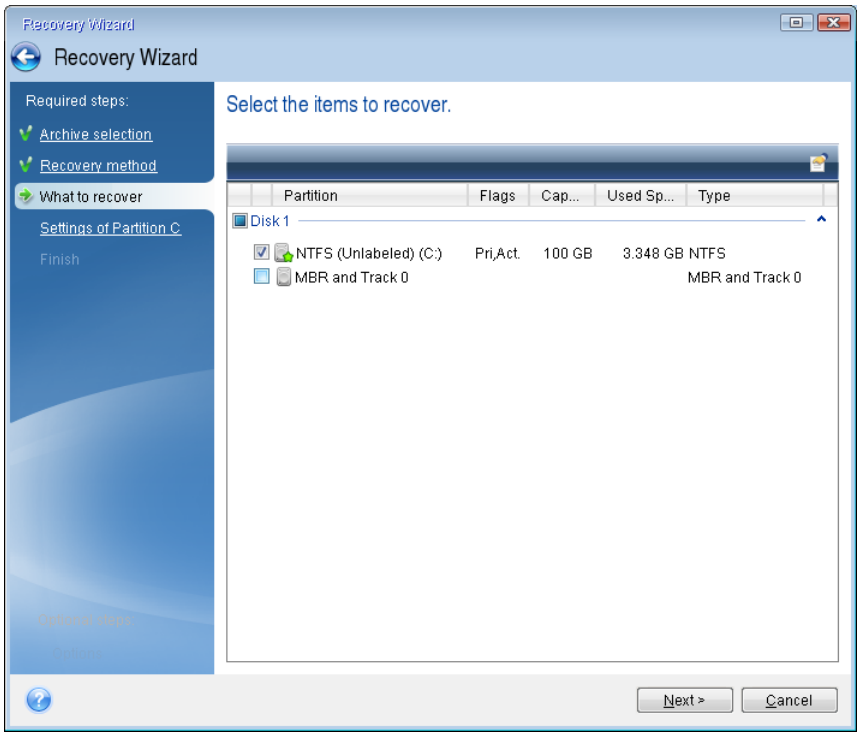


5. Select the system disk or partition backup to be used for recovery.
   When the backup is not displayed, click **Browse** and specify path to the backup manually.
6. Select **Recover whole disks and partitions** at the **Recovery method** step.



Copyright © Acronis International GmbH, 2002-2016

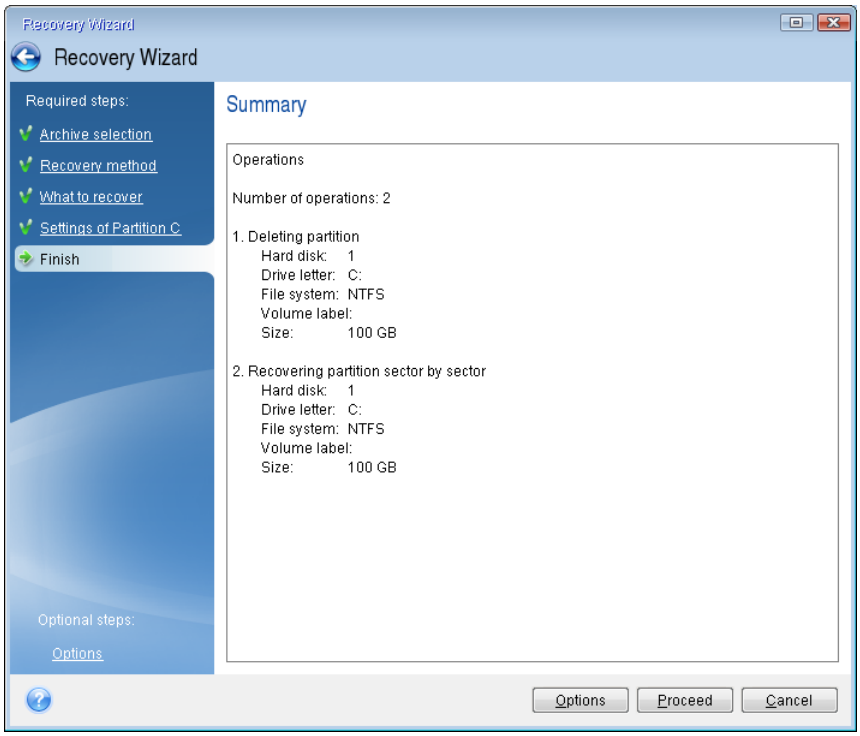
7. Select the system partition (usually C) on the **What to recover** screen. If the system partition has a different letter, select the partition using the **Flags** column. It must have the **Pri**, **Act** flags. If you have the System Reserved partition, select it, too.



8. At the "Settings of partition C" (or the letter of the system partition, if it is different) step check the default settings and click **Next** if they are correct. Otherwise, change the settings as required before clicking **Next**. Changing the settings will be needed when recovering to the new hard disk of a different capacity.

Copyright © Acronis International GmbH, 2002-2016

9. Carefully read the summary of operations at the **Finish** step. If you have not resized the partition, the sizes in the **Deleting partition** and **Recovering partition** items must match. Having checked the summary click **Proceed**.



10. When the operation finishes, exit the standalone version of Acronis True Image, remove the rescue media and boot from the recovered system partition. After making sure that you have recovered Windows to the state you need, restore the original boot order.

5.1.1.4 Recovering your system to a new disk under bootable media

Before you start, we recommend that you complete the preparations described in Preparing for recovery (p. 70). You do not need to format the new disk, as this will be done in the process of recovery.

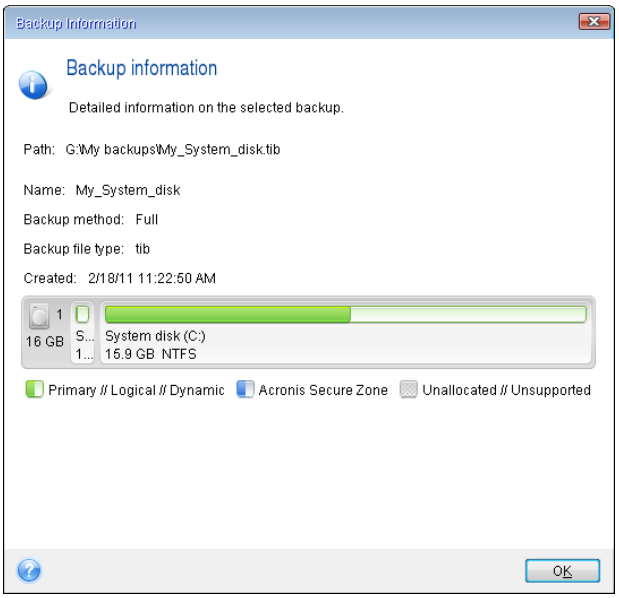
Warning! Your old and new hard drives must work in the same controller mode (for example, IDE or AHCI). Otherwise, your computer will not start from the new hard drive.

To recover your system to a new disk:

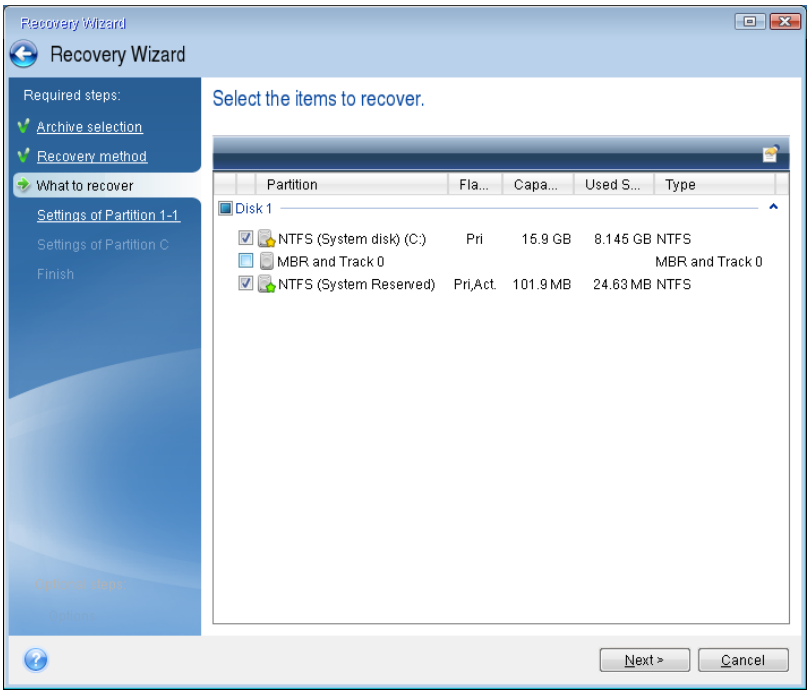
1. Install the new hard drive to the same position in the computer and use the same cable and connector that was used for the original drive. If this is not possible, install the new drive to where it will be used.
2. Attach the external drive if it contains the backup to be used for recovery and make sure that the drive is powered on.
3. Arrange the boot order in BIOS so as to make your rescue media device (CD, DVD or USB stick) the first boot device. See Arranging boot order in BIOS (p. 81).
4. Boot from the rescue media and select **Acronis True Image**.
5. On the **Home** screen, select **My disks** below **Recover**.
6. Select the system disk or partition backup to be used for recovery. When the backup is not displayed, click **Browse** and specify path to the backup manually.

Copyright © Acronis International GmbH, 2002-2016

7. If you have a hidden partition (for example, the System Reserved partition or a partition created by the PC manufacturer), click **Details** on the wizard's toolbar. Please remember the location and size of the hidden partition, because these parameters need to be the same on your new disk.



8. Select **Recover whole disks and partitions** at the **Recovery method** step.
9. On the **What to recover** step, select the boxes of the partitions to be recovered. Do not select the **MBR and Track 0** box.

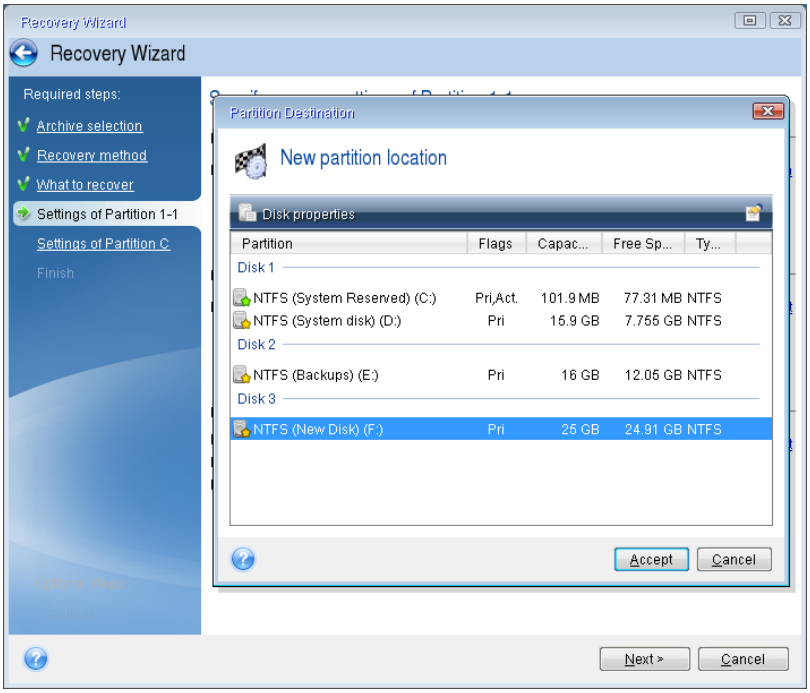


Selecting partitions leads to appearance of the relevant steps "Settings of partition ...". Note that these steps start with partitions which do not have an assigned disk letter (as usually is the case with hidden partitions). The partitions then take an ascending order of partition disk letters. This order cannot be changed. The order may differ from the physical order of the partitions on the hard disk.

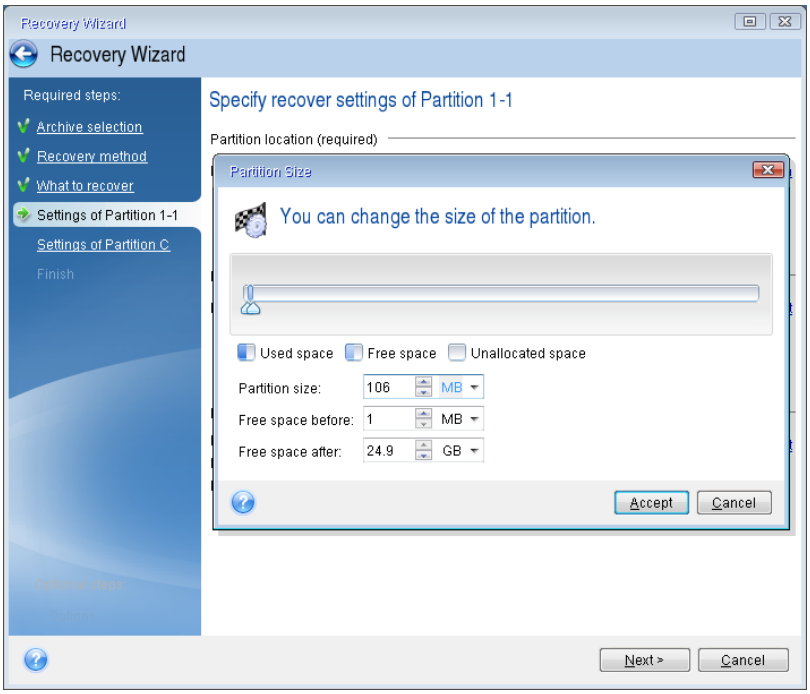
10. On the Settings of the hidden partition step (usually named Settings of Partition 1-1), specify the following settings:

Copyright © Acronis International GmbH, 2002-2016

- **Location.** Click **New location**, select your new disk by either its assigned name or capacity, and then click **Accept**.



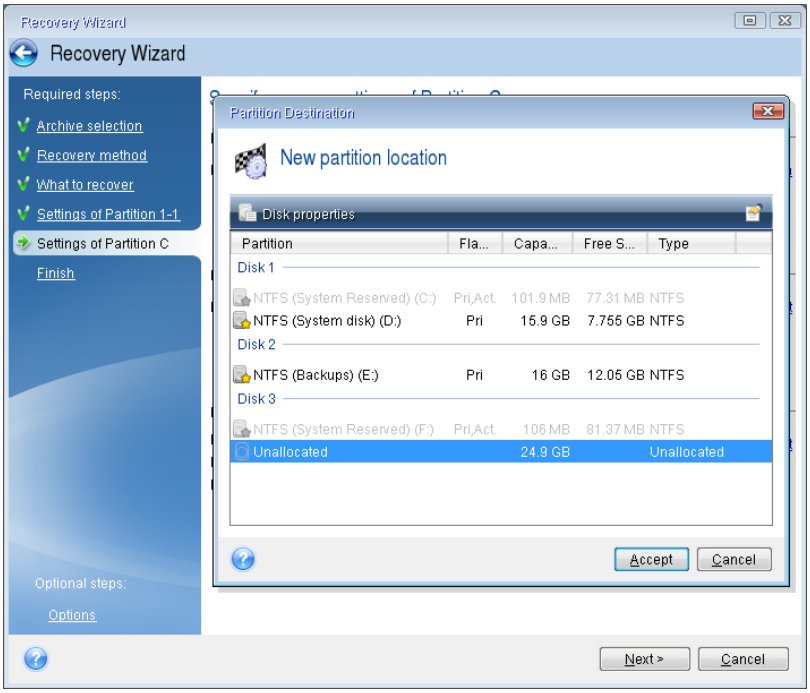
- **Type.** Check the partition type and change it, if necessary. Ensure that the System Reserved partition (if any) is primary and marked as active.
- **Size.** Click **Change default** in the Partition size area. By default the partition occupies the entire new disk. Enter the correct size in the Partition size field (you can see this value on the **What to recover** step). Then drag this partition to the same location that you saw in the Backup Information window, if necessary. Click **Accept**.



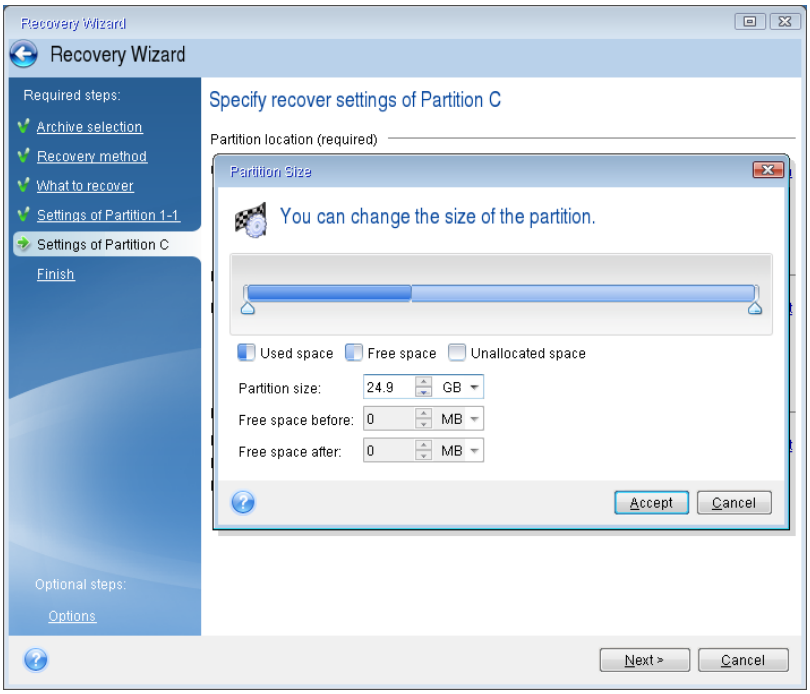
11. On the **Settings of Partition C** step, specify the settings for the second partition, which in this case is your system partition.

Copyright © Acronis International GmbH, 2002-2016

- Click **New location**, and then select unallocated space on the destination disk that will receive the partition.



- Change the partition type, if necessary. The system partition must be primary.
- Specify the partition size, which by default equals the original size. Usually there is no free space after the partition, so allocate all the unallocated space on the new disk to the second partition. Click **Accept**, and then click **Next**.



12. Carefully read the summary of operations to be performed and then click **Proceed**.

If your original disk contains a hidden partition created by the PC manufacturer, please proceed to MBR recovery. You need to recover the MBR because the PC manufacturer could change the generic Windows MBR or a sector on track 0 to provide access to the hidden partition.

Copyright © Acronis International GmbH, 2002-2016

1. Select the same backup again. Right-click and select **Recover** in the shortcut menu. Choose **Recover whole disks and partitions** at the Recovery method step and then select the **MBR and Track 0** box.
2. At the next step, select the destination disk as the target for MBR recovery. You can also recover the disk signature. Refer to Selecting target disk for MBR recovery (p. 77) for details.

   Click **Next** and then **Proceed**. After MBR recovery is complete, exit the standalone version of Acronis True Image.

When the recovery is complete

Before you boot the computer, please disconnect the old drive (if any). If Windows "sees" both the new and old drive during the boot, this will result in problems booting Windows. If you upgrade the old drive to a larger capacity new one, disconnect the old drive before the first boot.

Remove the rescue media and boot the computer to Windows. It may report that new hardware (hard drive) is found and Windows needs to reboot. After making sure that the system operates normally, restore the original boot order.

Acronis Universal Restore

When you recover your system to dissimilar hardware, the target computer could fail to boot. This is because the new hardware is incompatible with critical drivers included in the image. Acronis Universal Restore will help you make the target computer bootable. Refer to Acronis Universal Restore (p. 157) for details.

Selecting target disk for MBR recovery

In this window you should select a hard disk for recovering the Master Boot Record (MBR) along with track 0.

Recover disk signature check box

If you have selected MBR recovery at the **Content selection** step, the **Recover disk signature** check box will be in the bottom left corner. Disk signature is a part of a hard disk MBR. It is used for uniquely identifying the disk media.

We recommend that you select the **Recover disk signature** check box due to the following reasons:

- Acronis True Image creates scheduled tasks using the signature of the source hard disk. If you recover the same disk signature, you don't need to re-create or edit the tasks created previously.
- Some installed applications use a disk signature for licensing and other purposes.
- If you use Windows Restore Points, they will be lost when the disk signature is not recovered.
- Recovering a disk signature allows recovering VSS snapshots used by Windows Vista and Windows 7's "Previous Versions" feature.

We recommend that you clear the **Recover disk signature** check box when:

- You use an image backup not for disaster recovery but for cloning your Windows hard drive to another one.

In this case, Acronis True Image generates a new disk signature for the recovered hard drive, even if you recover to the same drive.

Copyright © Acronis International GmbH, 2002-2016

Having selected a hard disk drive and specified whether to recover the disk signature, click **Next** to continue.

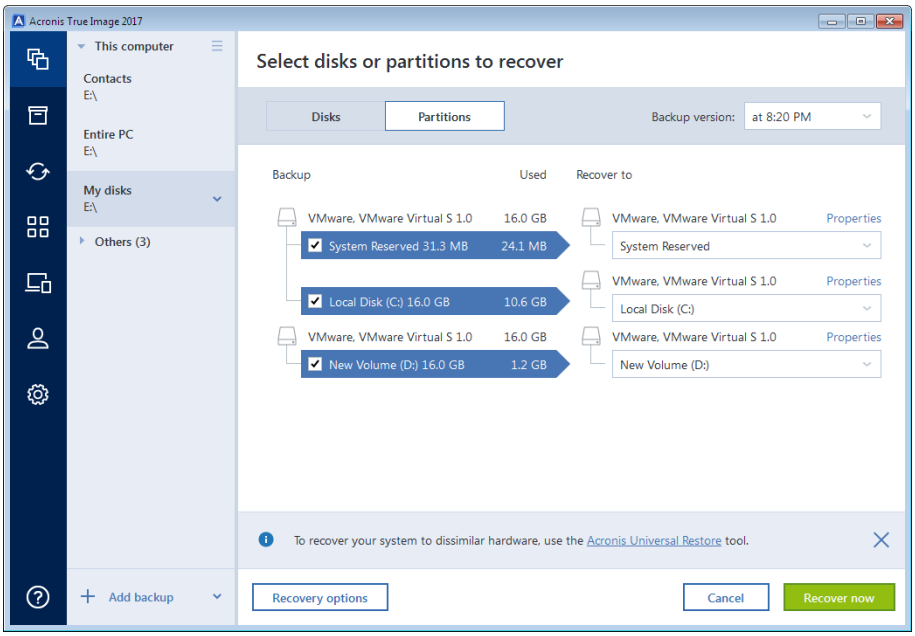
5.1.2 Recovering partitions and disks

You can recover your disks from backups located on local storage, network storage, or Acronis Cloud.

Depending on your Internet connection speed, disk recovery from Acronis Cloud may take a long time.

To recover partitions or disks:

1. Start Acronis True Image.
2. If you want to recover your data from Acronis Cloud, make sure that you are signed in to your Acronis account.
3. In the **Backup** section, select the backup which contains the partitions or disks you want to recover, and then click **Recover disks**.
4. In the **Backup version** list, select the backup version you want to recover by its backup date and time.



5. Select the disks to recover.

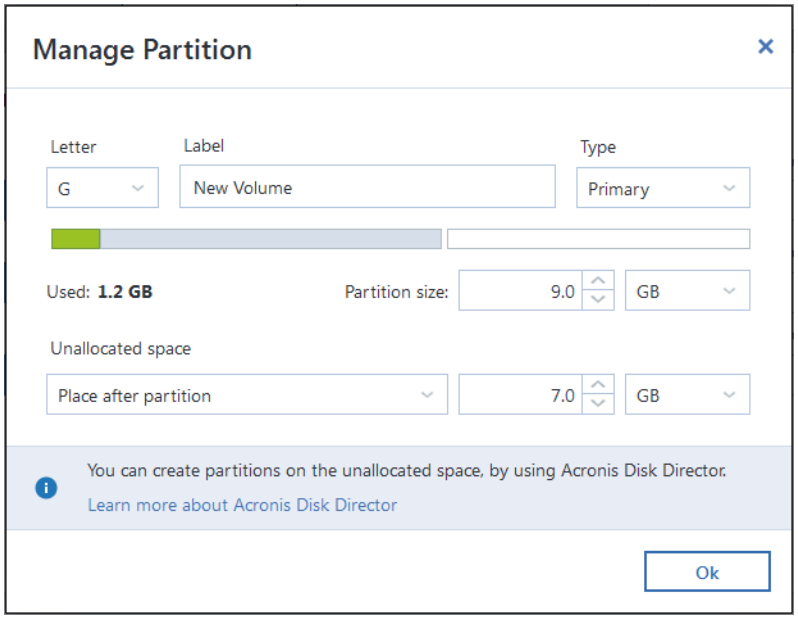
   If you need to recover separate partitions, click **Recover specific partitions**, and then select the partitions to recover.
6. In the recovery destination field below the partition name, select the destination partition. Unsuitable partitions are marked by red lettering. Note that all data on the destination partition will be lost because it is replaced by the recovered data and file system.

   *To recover to the original partition, at least 5 % of the partition space must be free. Otherwise, the **Recover now** button will be unavailable.*
7. [optional step] To set up additional parameters for the disk recovery process, click **Options**.
8. After you finish with your selections, click **Recover now** to start recovery.

Copyright © Acronis International GmbH, 2002-2016

5.1.2.1 Partition properties

When you recover partitions to a basic disk, you can change properties of these partitions. To open the **Partition Properties** window, click **Properties** next to the selected target partition.



You can change the following partition properties:

- **Letter**
- **Label**
- **Type**

  You can make the partition primary, primary active, or logical.
- **Size**

  You can resize the partition by dragging the right-side border with your mouse, on the horizontal bar on the screen. To assign the partition a specific size, enter the appropriate number into the **Partition size** field. You can also select the position of unallocated space—before or after the partition.

5.1.3 About recovery of dynamic/GPT disks and volumes

Recovery of dynamic volumes

You can recover dynamic volumes to the following locations on the local hard drives:

- **Dynamic volume.**

  Manual resizing of dynamic volumes during recovery to dynamic disks is not supported. If you need to resize a dynamic volume during recovery, it should be recovered to a basic disk.

  - **Original location (to the same dynamic volume).**

    The target volume type does not change.
  - **Another dynamic disk or volume.**

    The target volume type does not change. For example, when recovering a dynamic striped volume over a dynamic spanned volume the target volume remains spanned.
  - **Unallocated space of the dynamic group.**

    The recovered volume type will be the same as it was in the backup.

Copyright © Acronis International GmbH, 2002-2016

- **Basic volume or disk.**

  The target volume remains basic.
- **Bare-metal recovery.**

  When performing a so called "bare-metal recovery" of dynamic volumes to a new unformatted disk, the recovered volumes become basic. If you want the recovered volumes to remain dynamic, the target disks should be prepared as dynamic (partitioned and formatted). This can be done using third-party tools, for example, Windows Disk Management snap-in.

Recovery of basic volumes and disks

- When recovering a basic volume to an unallocated space of the dynamic group, the recovered volume becomes dynamic.
- When recovering a basic disk to a dynamic disk of a dynamic group consisting of two disks, the recovered disk remains basic. The dynamic disk to which the recovery is performed becomes "missing" and a spanned/striped dynamic volume on the second disk becomes "failed".

Partition style after recovery

The target disk's partition style depends on whether your computer supports UEFI and on whether your system is BIOS-booted or UEFI-booted. See the following table:

	My system is BIOS-booted (Windows or Acronis Bootable Media)	My system is UEFI-booted (Windows or Acronis Bootable Media)
My source disk is MBR and my OS does not support UEFI	The operation will not affect neither partition layout nor bootability of the disk: partition style will remain MBR, the destination disk will be bootable in BIOS.	After operation completion, the partition style will be converted to GPT style, but the operating system will fail booting from UEFI, since your operating system does not support it.
My source disk is MBR and my OS supports UEFI	The operation will not affect neither partition layout nor bootability of the disk: partition style will remain MBR, the destination disk will be bootable in BIOS.	The destination partition will be converted to GPT style that will make the destination disk bootable in UEFI. See Example of recovery to UEFI system (p. 80).
My source disk is GPT and my OS supports UEFI	After operation completion, the partition style will remain GPT, the system will fail booting on BIOS, because your operating system cannot support booting from GPT on BIOS.	After operation completion, the partition style will remain GPT, the operating system will be bootable on UEFI.

Example of recovery procedure

See Example of recovery to a UEFI system (p. 80).

5.1.3.1 Example of recovery to a UEFI system

Here is an example for transferring a system with the following conditions:

- The source disk is MBR and the OS supports UEFI.
- The target system is UEFI-booted.
- Your old and new hard drives work in the same controller mode (for example, IDE or AHCI).

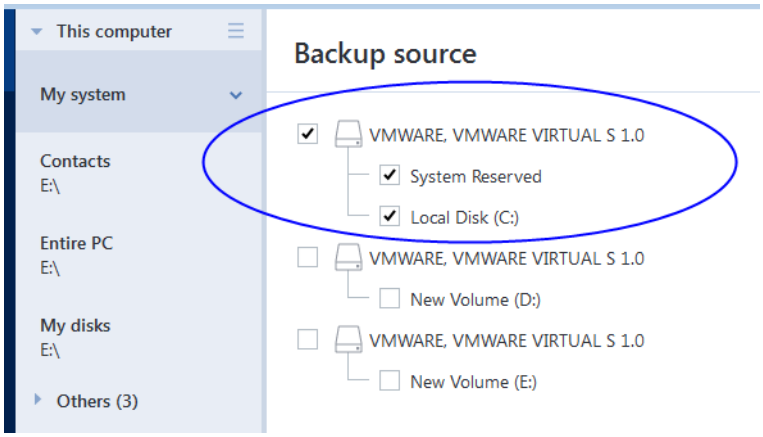
Copyright © Acronis International GmbH, 2002-2016

Before you start the procedure, please ensure that you have:

- **Bootable rescue media.**

  Refer to Creating bootable rescue media (p. 17) for details.
- **Backup of your system disk created in disk mode.**

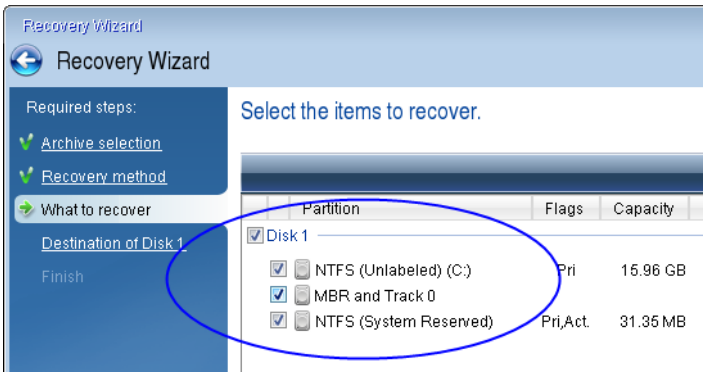
  To create this backup, switch to disk mode, and then select the hard drive that contains your system partition. Refer to Backing up disks and partitions (p. 41) for details.



To transfer your system from an MBR disk to a UEFI-booted computer:

1. Boot from the rescue media in UEFI mode and select Acronis True Image.
2. Run the **Recovery wizard** and follow the instructions described in Recovering your system (p. 70).
3. On the **What to recover** step, select the check box next to the disk name to select the entire system disk.

   In the example below, you need to select the **Disk 1** check box:



4. On the **Finish** step, click **Proceed**.

When the operation finishes, the destination disk is converted to GPT style so that it is bootable in UEFI.

After the recovery, please ensure that you boot your computer in UEFI mode. You may need to change the boot mode of your system disk in the user interface of the UEFI boot manager.

5.1.4 Arranging boot order in BIOS

To boot your computer from Acronis bootable rescue media, you need to arrange boot order in BIOS so the media is the first booting device.

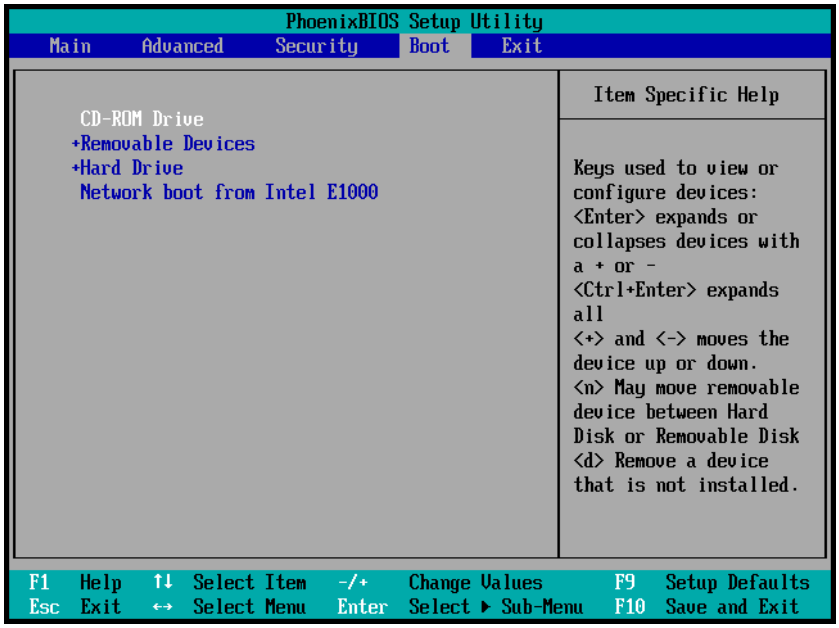
Copyright © Acronis International GmbH, 2002-2016

To boot from Acronis bootable media:

1. If you use a USB flash drive as a bootable media, plug it into the USB port.
2. Turn your computer on. During the Power-On Self Test (POST), you will see the key combination that you need to press in order to enter BIOS.
3. Press the key combination (such as, **Del, F1, Ctrl+Alt+Esc, Ctrl+Esc**). BIOS setup utility will open. Note that BIOS may differ in appearance, sets of items, names, etc.

   *Some motherboards have a so called boot menu opened by pressing a certain key or key combination, for instance, **F12**. The boot menu allows selecting the boot device from a list of bootable devices without changing the BIOS setup.*

4. If you use a CD or DVD as a bootable media, insert it in the CD or DVD drive.
5. Make your rescue media (CD, DVD or USB drive) device the first booting device:
   1. Navigate to the Boot order setting by using the arrow keys on your keyboard.
   2. Place the pointer on the device of your bootable media and make it the first item in the list. You can usually use the Plus Sign and the Minus Sign keys to change the order.


PhoenixBIOS Setup Utility
Main
Advanced
Security
Boot
Exit
CD-ROM Drive
+Removable Devices
+Hard Drive
Network boot from Intel E1000
Item Specific Help
Keys used to view or configure devices:
<Enter> expands or collapses devices with a + or -
<Ctrl+Enter> expands all
<+> and <-> moves the device up or down.
<n> May move removable device between Hard Disk or Removable Disk
<d> Remove a device that is not installed.
F1 Help ↑↓ Select Item -/+ Change Values F9 Setup Defaults
Esc Exit ↔ Select Menu Enter Select ▸ Sub-Menu F10 Save and Exit

6. Exit BIOS and save the changes that you made. The computer will boot from Acronis bootable media.

If the computer fails to boot from the first device, it tries to boot from the second device in the list, and so on.

5.2 Recovering files and folders

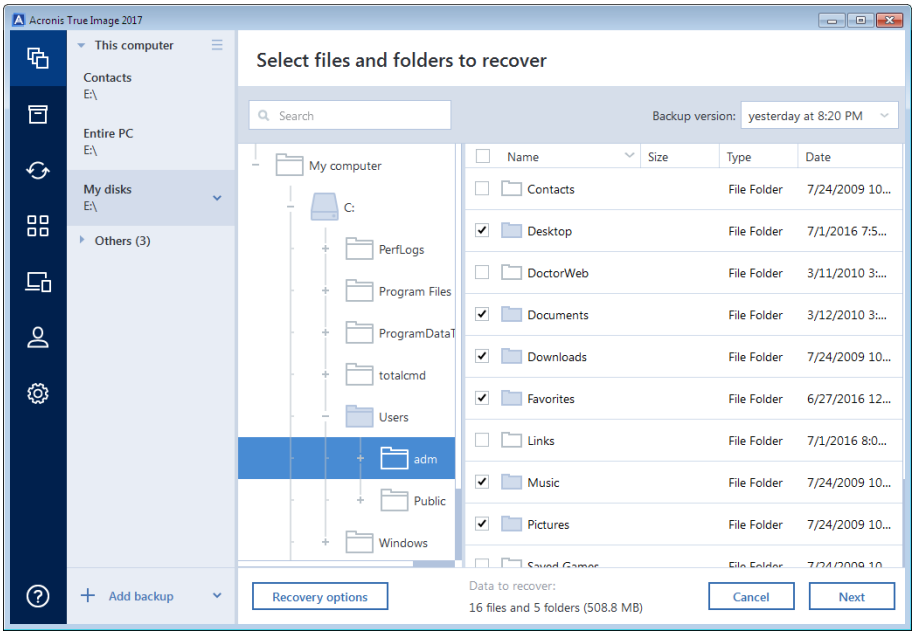
You can recover files and folders both from file-level and disk-level backups.

To recover files and folders:

1. Start Acronis True Image.
2. On the sidebar, click **Backup**.
3. From the backup list, select the backup which contains the files or folders that you want to recover.
4. On the right panel, click **Recover files**.

Copyright © Acronis International GmbH, 2002-2016

5. Select backup version (data state on specific date and time).
6. Select the files and folders that you want to recover, and then click **Next**.



7. Select a destination on your computer to where you want to recover selected files/folders. You can recover data to its original location or choose a new one, if necessary. To choose a new location, click the **Browse** button.

   When you choose a new location, the selected items will be recovered by default without recovering the original, absolute path. You may also wish to recover the items with their entire folder hierarchy. In this case select the **Keep the original folder structure** check box.
8. When needed, set the options for the recovery process (recovery process priority, file-level security settings, etc.). To set the options, click **Options**. The options you set here will be applied only to the current recovery operation.
9. To start the recovery process, click the **Recover now** button.

   You can stop the recovery by clicking **Cancel**. Please keep in mind that the aborted recovery may still cause changes in the destination folder.

Recovering files in File Explorer

To recover files and folders directly from File Explorer:

1. Double-click the corresponding .tib file, and then browse to the file or folder that you want to recover.
2. Copy the file or folder to a hard disk.

Note: The copied files lose the "Compressed" and "Encrypted" attribute. If you need to keep these attributes, it is recommended to recover the backup.

5.3 Searching backup content

While recovering data from local backups, you can search for specific files and folders stored in the selected backup.

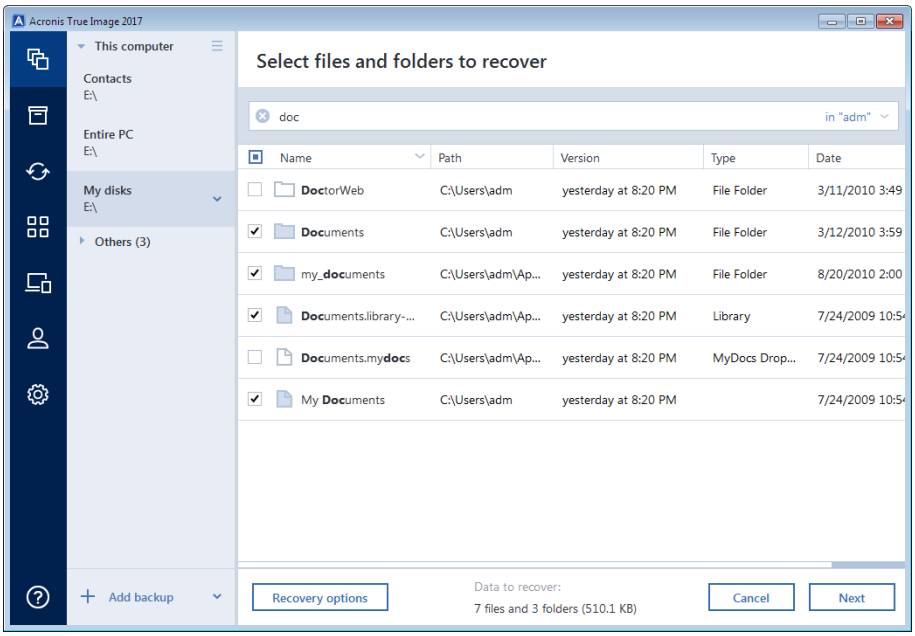
Note: Acronis True Image cannot perform search in Acronis Cloud.

Copyright © Acronis International GmbH, 2002-2016

To search for files and folders:

1. Start recovering data as described in Recovering partitions and disks (p. 78) or Recovering files and folders (p. 82).
2. When selecting files and folders to recover, enter the file or folder name into the **Search** field. The program shows search results.

   You can also use the common Windows wildcard characters: * and ?. For example, to find all files with extension **.exe**, enter ***.exe**. To find all .exe files with names consisting of five symbols and starting with "my", enter **My???.exe**.



3. By default, Acronis True Image searches the folder selected on the previous step. To include the entire backup in the search, click the down arrow, and then click **in entire backup**.

   To return to the previous step, delete the search text, and then click the cross icon.
4. After the search is complete, select the files that you want to recover, and then click **Next**.

Note: Pay attention to the Version column. The files and folders that belong to different backup versions cannot be recovered at the same time.

5.4 Recovery from Acronis Cloud

In this section

Recovering data from online backups 84
Selecting a version to recover.....85
Disk recovery from Cloud.....86

5.4.1 Recovering data from online backups

With Acronis True Image you can browse and recover data that was backed up on Acronis Cloud. If you have backed up data from several computers, select the online backup box for the computer from which you backed up the data you want to recover.

To recover files and folders from Acronis Cloud:

1. Start Acronis True Image.

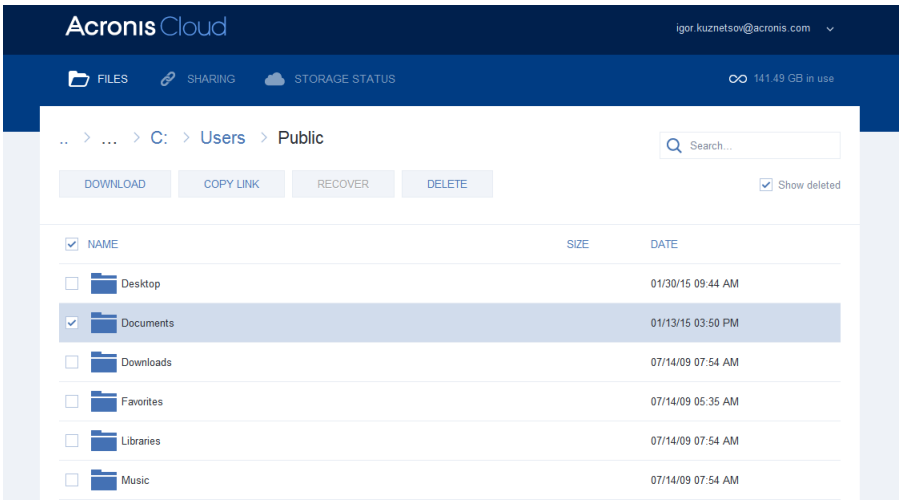
Copyright © Acronis International GmbH, 2002-2016

2. On the sidebar, click **Backup**.
3. From the backup list, select the backup which contains the files or folders that you want to recover.
4. On the right panel, click **Recover files**.

   You will be taken to Acronis Cloud website.

   If the data from the selected computer is stored on the Cloud in encrypted form, you will be asked to enter the password which has been used for encryption. You will not be able to access the data until you enter the correct password.

5. After the **Files** tab on the Acronis Cloud website opens, select the required online backup in the **Backups** area.
6. Select the files and folders you want to recover. Click the **Download** button to start recovery.



If you selected several files and folders, they will be placed into a zip archive.

By default the data will be downloaded to the **Downloads** folder. You may change the download path.

5.4.2 Selecting a version to recover

By default Acronis True Image selects the latest versions with respect to the date you specified. However, for any file you can select a specific version of the file to recover.

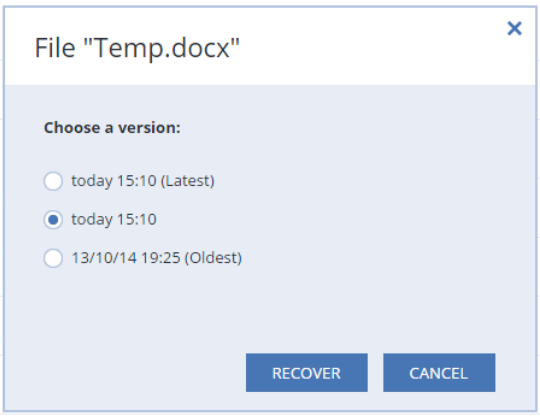
Note that this option is not applicable to folders.

To recover a specific file version:

1. In the backup contents, select the file which version you want to recover, then click the gear icon at the right-hand side. Select **View versions** in the opened menu.

Copyright © Acronis International GmbH, 2002-2016

2. In the window that appears, select the required version and then click **Recover**.



3. Select the version to which you want to rollback. The version's exact date and time will be displayed. Your current version will be reverted to the state it was at that point in time.
4. Click **Recover** to proceed. The selected version will become the latest version on Acronis Cloud.
5. After the process finishes, refresh the **Files** page in your web browser.
6. Select the file once more and then click **Download** to download the selected version to your Downloads folder.

5.4.3 Disk recovery from Cloud

Disk recovery from Acronis Cloud is very similar to the recovery from an ordinary hard disk drive.

- When you can start Windows and Acronis True Image, please refer to Recovering partitions and disks (p. 78).
- When Windows cannot start, please refer to Recovering your system from Acronis Cloud (p. 87).

How it works

Your computer should be connected to the Internet either by an Ethernet cable or via Wi-Fi. Acronis True Image supports several wireless security protocols, including WPA-Personal, WPA2-Personal, and WPA2-Enterprise.

Recovery to the original location

When you recover a disk to the original location, Acronis True Image does not download the entire disk space to your computer. It scans your disk searching for data changes and recovers only those files that are different from files in the image. This technology significantly reduces the amount of data you need to download in order to recover your disk.

Recovery to a new location

When you recover a disk to a different location or to an unallocated space, the process is very similar to a recovery from a local storage. The only difference is in the data writing method. Acronis True Image downloads and writes data by separate blocks, and not continuously. This technology increases recovery speed and reliability of the entire process.

What if recovery has been interrupted

Since disk recovery from Acronis Cloud uses an Internet connection and usually takes a long time, the probability of the recovery interruption is higher comparing to recovery from an ordinary hard disk.

Possible reasons of recovery interruption:

Copyright © Acronis International GmbH, 2002-2016

- Internet connection has been lost.
- Connection to Acronis Cloud has been lost.
- You canceled the recovery, deliberately or accidentally.
- Electricity supply problem.

When recovery is not complete due to a connection problem, Acronis True Image automatically tries to reconnect to Acronis Cloud and resume the recovery process. It is recommended that you check your Internet connection settings in this case. If all the automatic attempts fail, run the recovery again manually when connection is restored.

In other cases please run recovery again manually and make sure the recovery is complete.

Regardless of an interruption reason, Acronis True Image does not start recovery from the very beginning. It resumes the process and downloads only the data that was not recovered.

5.4.3.1 Recovering your system from Acronis Cloud

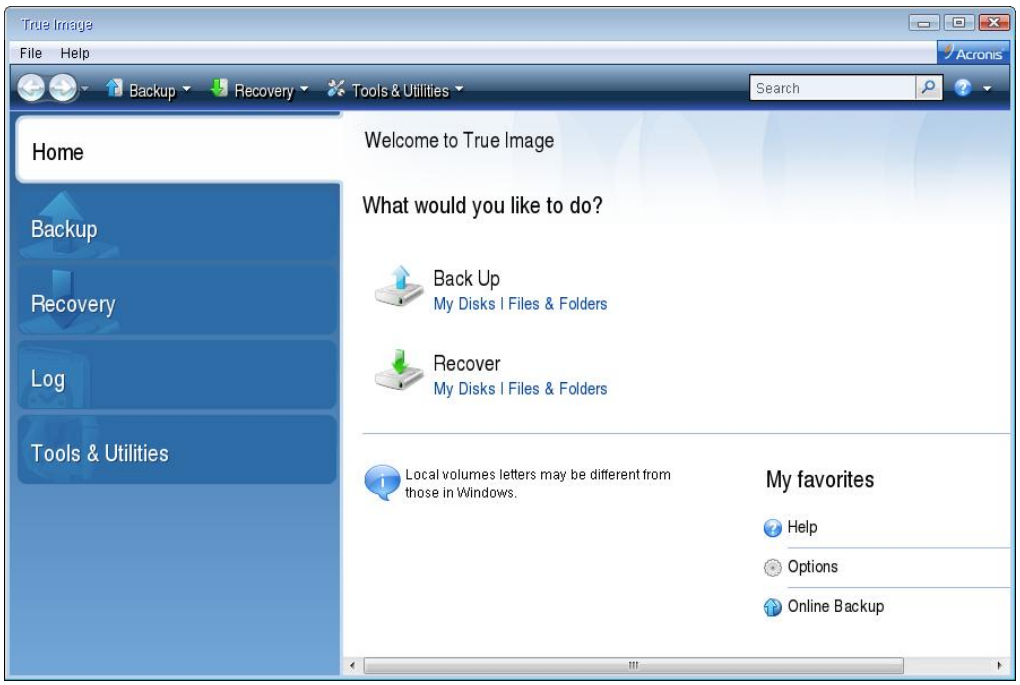
Depending on your Internet connection speed, disk recovery from Acronis Cloud may take a long time.

Before you start, we recommend that you complete the preparations described in Preparing for recovery (p. 70). If you recover your system to a new disk, you do not need to format the new disk, as this will be done in the process of recovery.

Before starting this procedure, please make sure that your computer is connected to the Internet by an Ethernet cable or over Wi-Fi.

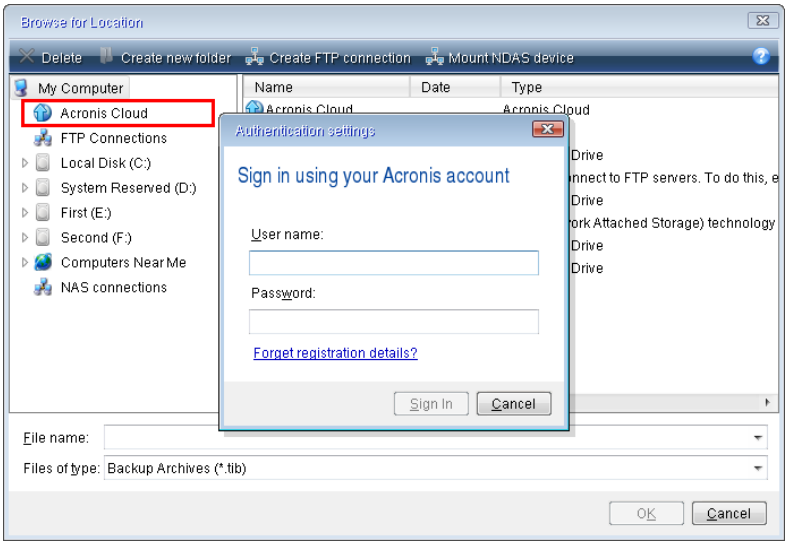
To recover a system disk from Acronis Cloud:

1. Arrange the boot order in BIOS so as to make your rescue media device (CD, DVD or USB stick) the first boot device. See Arranging boot order in BIOS (p. 81).
2. Boot from the rescue media and select **Acronis True Image**.
3. On the **Home** screen, select **My disks** below **Recover**.

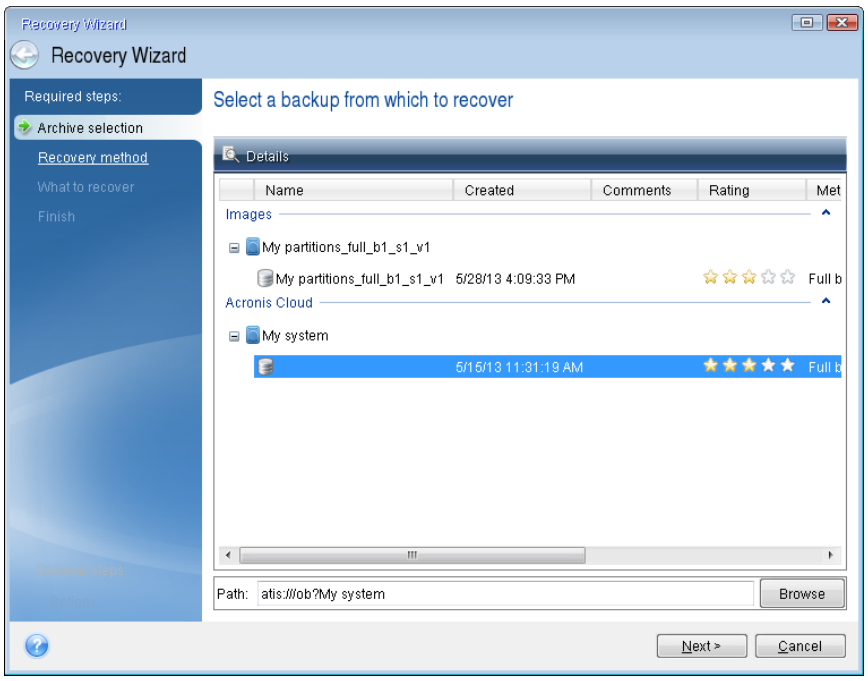


Copyright © Acronis International GmbH, 2002-2016

4. To add the online backup of the system disk or system partition to the list of available backups, click **Browse**.
5. In the directory tree of the opened window, select Acronis Cloud and enter credentials of your Acronis account.



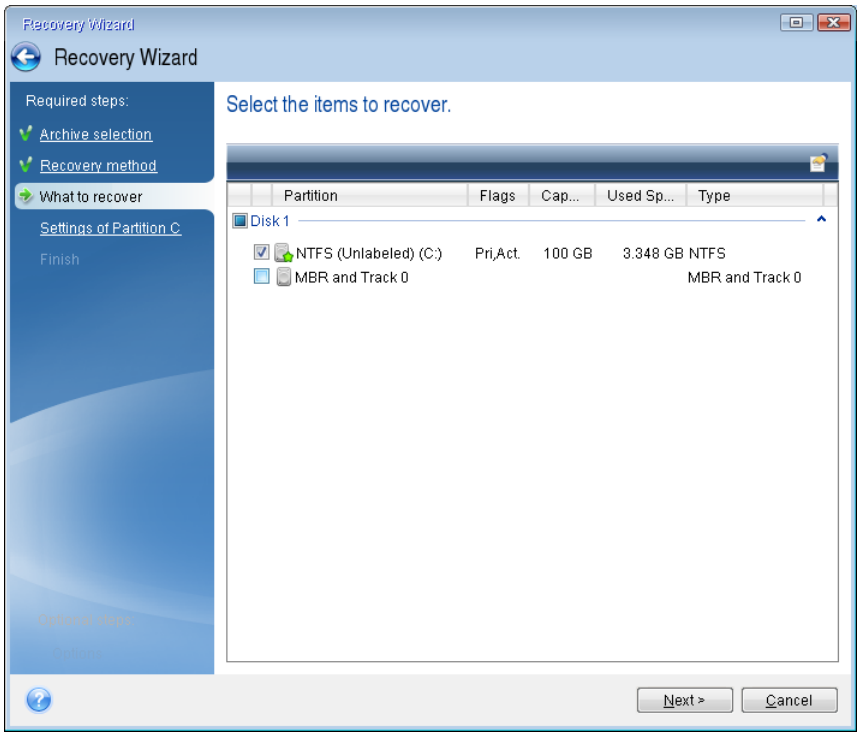
6. Select the backup you want to use for recovery, and click **OK**.
7. On the **Archive selection** step, select the online backup and click **Next**.



8. On the **Recovery method** step, select **Recover whole disks and partitions**.

Copyright © Acronis International GmbH, 2002-2016

9. On the **What to recover** step, select the system partition (usually C) and the System Reserved partition (if any). You can also recognize these partitions by the **Pri**, **Act** flags.



10. On the "Settings of partition C" (or the letter of the system partition, if it is different) step, change the settings, if necessary. For example, you need to change settings when recovering to the new hard disk of a different capacity.
11. Carefully read the summary of operations at the **Finish** step. If you have not resized the partition, the sizes in the **Deleting partition** and **Recovering partition** items must match. Click **Proceed**.
12. When recovery is complete, exit the standalone version of Acronis True Image, remove the rescue media. Boot from the recovered system partition. After you check that you have recovered Windows to the state you need, restore the original boot order.

5.5 Recovery options

You can configure options for the disk/partition and file recovery processes. After you installed the application, all options are set to the initial values. You can change them for your current recovery operation only or for all further recovery operations as well. Select the **Save the settings as default** check box to apply the modified settings to all further recovery operations by default.

Note, that disk recovery options and file recovery options are fully independent, and you should configure them separately.

If you want to reset all the modified options to their initial values that were set after the product installation, click the **Reset to initial settings** button.

In this section

Disk recovery mode 90
Pre/Post commands for recovery 90
Validation option.....90
Computer restart 91
File recovery options.....91

Copyright © Acronis International GmbH, 2002-2016

Overwrite file options 91
Performance of recovery operation 92
Notifications for recovery operation 92

5.5.1 Disk recovery mode

With this option you can select the disk recovery mode for image backups.

- **Recover sector-by-sector** - select this check box if you want to recover both used and unused sectors of disks or partitions. This option will be effective only when you choose to recover a sector-by-sector backup.

5.5.2 Pre/Post commands for recovery

You can specify commands (or even batch files) that will be automatically executed before and after the recovery procedure.

For example, you may want to start/stop certain Windows processes, or check your data for viruses before recovery.

To specify commands (batch files):

- Select a command to be executed before the recovery process starts in the **Pre-command** field. To create a new command or select a new batch file, click the **Edit** button.
- Select a command to be executed after the recovery process ends in the **Post-command** field. To create a new command or select a new batch file, click the **Edit** button.

Please do not try to execute interactive commands, i.e. commands that require user input (for example, "pause"). These are not supported.

5.5.2.1 Edit user command for recovery

You can specify user commands to be executed before or after recovery:

- In the **Command** field type-in a command or select it from the list. Click **...** to select a batch file.
- In the **Working directory** field type-in a path for command execution or select it from the list of previously entered paths.
- In the **Arguments** field enter or select command execution arguments from the list.

Disabling the **Do not perform operations until the command execution is complete** parameter (enabled by default), will permit the recovery process to run concurrently with your command execution.

The **Abort the operation if the user command fails** (enabled by default) parameter will abort the operation if any errors occur in command execution.

You can test the command you entered by clicking the **Test command** button.

5.5.3 Validation option

- **Validate backup before recovery**—Enable this option to check the backup integrity before recovery.
- **Check the file system after recovery**—Enable this option to check the file system integrity on the recovered partition.

Only FAT16/32 and NTFS file systems can be checked.

 Copyright © Acronis International GmbH, 2002-2016

The file system will not be checked if a reboot is required during recovery, for example, when recovering the system partition to its original place.

5.5.4 Computer restart

If you want the computer to reboot automatically when it is required for recovery, select the **Restart the computer automatically if needed for the recovery** check box. This may be used when a partition locked by the operating system has to be recovered.

5.5.5 File recovery options

You can select the following file recovery options:

- **Recover files with their original security settings** - if the file security settings were preserved during backup (see File-level security settings for backup (p. 60)), you can choose whether to recover them or let the files inherit the security settings of the folder where they will be recovered to. This option is effective only when recovering files from file/folder backups.
- **Set current date and time for recovered files** - you can choose whether to recover the file date and time from the backup or assign the files the current date and time. By default the file date and time from the backup will be assigned.

5.5.6 Overwrite file options

Choose what to do if the program finds a file in the target folder with the same name as in the backup.

This option is available only while restoring data from file-level backups.

Selecting the **Overwrite existing files** check box will give the files from the backup unconditional priority over the files on the hard disk, though, by default, the more recent files and folders are protected against overwriting. If you want to overwrite those files and folders too, clear the appropriate check box.

If you do not need to overwrite some files:

- Select/clear the **Hidden files and folders** check box to enable/disable overwriting of all hidden files and folders.
- Select/clear the **System files and folders** check box to enable/disable overwriting of all system files and folders.
- Select/clear the **More recent files and folders** check box to enable/disable overwriting of new files and folders.
- Click **Add specific files and folders** to manage the list of custom files and folders that you do not want to overwrite.
  - To disable overwriting of specific files, click the **Add...** button to create an exclusion criterion.
  - While specifying the criteria, you can use the common Windows wildcard characters. For example, to preserve all files with extension **.exe**, you can add ***.exe**. Adding **My???.exe** will preserve all .exe files with names consisting of five symbols and starting with “my”.

To delete a criterion, for example, added by mistake, click the Delete icon to the right of the criterion.

Copyright © Acronis International GmbH, 2002-2016

5.5.7 Performance of recovery operation

On the **Performance** tab you can configure the following settings:

Operation priority

Changing the priority of a backup or recovery process can make it run faster or slower (depending on whether you raise or lower the priority), but it can also adversely affect the performance of other running programs. The priority of any process running in a system, determines the amount of CPU usage and system resources allocated to that process. Decreasing the operation priority will free more resources for other CPU tasks. Increasing backup or recovery priority may speed up the process by taking resources from the other currently running processes. The effect will depend on total CPU usage and other factors.

You can set up the operation priority:

- **Low** (enabled by default) - the backup or recovery process will run slower, but the performance of other programs will be increased.
- **Normal** - the backup or recovery process will have the equal priority with other processes.
- **High** - the backup or recovery process will run faster, but the performance of other programs will be reduced. Be aware that selecting this option may result in 100% CPU usage by Acronis True Image.

5.5.8 Notifications for recovery operation

Sometimes a backup or recovery procedure can last an hour or longer. Acronis True Image can notify you when it is finished via e-mail. The program can also duplicate messages issued during the operation or send you the full operation log after operation completion.

By default all notifications are disabled.

Free disk space threshold

You may want to be notified when the free space on the backup storage becomes less than the specified threshold value. If after starting a backup Acronis True Image finds out that the free space in the selected backup location is already less than the specified value, the program will not begin the actual backup process and will immediately inform you by displaying an appropriate message. The message offers you three choices - to ignore it and proceed with the backup, to browse for another location for the backup or to cancel the backup.

If the free space becomes less than the specified value while the backup is being run, the program will display the same message and you will have to make the same decisions.

To set the free disk space threshold:

- Select the **Show notification message on insufficient free disk space** check box
- In the **Size** box, type or select a threshold value and select a unit of measure

Acronis True Image can monitor free space on the following storage devices:

- Local hard drives
- USB cards and drives
- Network shares (SMB/NFS)

*The message will not be displayed if the **Do not show messages and dialogs while processing (silent mode)** check box is selected in the **Error handling** settings.*

Copyright © Acronis International GmbH, 2002-2016

This option cannot be enabled for FTP servers and CD/DVD drives.

E-mail notification

You can specify an email account that will be used to send you email notifications.

To configure the email notifications:

1. Select the **Send e-mail notifications about the operation state** check box.
2. Configure email settings:
   - Enter the email address in the **To** field. You can enter several email addresses in a semicolon-delimited format.
   - Enter the outgoing mail server (SMTP) in the **Outgoing mail server (SMTP)** field.
   - Set the port of the outgoing mail server. By default the port is set to 25.
   - If required, select the **SMTP authentication** check box, and then enter the user name and password in the corresponding fields.
3. To check whether your settings are correct, click the **Send test message** button.

If the test message sending fails, then perform the following:

1. Click **Show extended settings**.
2. Configure additional email settings:
   - Enter the e-mail sender address in the **From** field. If you are not sure what address to specify, then type any address you like in a standard format, for example *aaa@bbb.com*.
   - Change the message subject in the **Subject** field, if necessary.
   - Select the **Log on to incoming mail server** check box.
   - Enter the incoming mail server (POP3) in the **POP3 server** field.
   - Set the port of the incoming mail server. By default the port is set to 110.
3. Click the **Send test message** button again.

Additional notification settings:

- To send a notification concerning process completion, select the **Send notification upon operation's successful completion** check box.
- To send a notification concerning process failure, select the **Send notification upon operation failure** check box.
- To send a notification with operation messages, select the **Send notification when user interaction is required** check box.
- To send a notification with full log of operations, select the **Add full log to the notification** check box.

Copyright © Acronis International GmbH, 2002-2016

6 Archiving data

In this section

What is data archiving?....94
What is excluded from archives?....95
Cloud archiving vs. Online backup....95
Archiving your data....96
Accessing your archived files....97

6.1 What is data archiving?

Data archiving is a tool that allows you to move your big or rarely used files to Acronis Cloud, NAS, an external hard drive, or a USB flash drive. Every time you run this tool, it analyzes the data in the selected folder and suggests uploading the found files to Acronis Cloud or moving them to local storage. You can select the files and folders that you want to archive. After moving to an archive, the local copies of these files will be deleted. The links to the files are stored in a special location called Acronis Archive. You can access the location as an ordinary folder in File Explorer. Double-clicking a file link will open the file as if it was stored in the local folder. If the file is archived to Acronis Cloud, it will be downloaded back to your computer, first. You can also access and manage it right in Acronis Cloud.

Data archiving has the following main features:

- **Free storage space saving**

  As a rule, storage space of modern high-capacity hard drives is mostly occupied by user data, such as photographs and documents, and not by the operating system or applications. Since most of the data is used occasionally, there is no need to keep them on a local drive. Data archiving helps you free up storage space for frequently used files.
- **Cloud archiving and local archiving**

  You can choose a destination type for your archive: Acronis Cloud or local storage, such as an internal hard drive, external hard drive, NAS, or a USB flash drive. Every time you choose Acronis Cloud as a destination, the selected data is stored in the same cloud archive. Local archives are independent from each other and may have different names, destinations, encryption settings, and so on, though you can select an existing archive as a destination instead of creating a new one. The number of local archives is not limited.
- **Easy access of cloud archive from any device**

  When you archive your files to Acronis Cloud, you can access them with Acronis True Image, the Acronis True Image mobile application, and the Acronis Cloud web application from any device running Windows, Mac OS X, iOS, and Android, including tablets and smartphones.
- **Data protection in the cloud archive**

  Your data stored in Acronis Cloud is protected from corruption or disaster. For example, in case of your local hard drive failure, you can download your files to your new hard drive. Moreover, your data is stored in encrypted state. You can be sure that no one except you can access your data.
- **File sharing**

  When your files are uploaded to Acronis Cloud, you can create public links to share the files with your friends or to post them to forums and social networks.
- **File versions**

Copyright © Acronis International GmbH, 2002-2016

For the files that have been changed and uploaded to Acronis Cloud several times, Acronis True Image keeps all the modifications in different file versions. You can choose a previous file version and download it to your device.

6.2 What is excluded from archives?

To reduce archive size and eliminate a possibility to corrupt your system, by default Acronis True Image excludes the following data from archives:

- pagefile.sys
- swapfile.sys
- The Temp folder
- The System Volume Information folder
- The Recycle Bin
- Web browser temporary data:
  - Temporary Internet files
  - Cache
- .tib files
- .tib.metadata files
- .tmp files
- .~ files

See the full file list in the Knowledge Base article: https://kb.acronis.com/content/58297.

6.3 Cloud archiving vs. Online backup

When you archive your data to Acronis Cloud, it is similar to an online backup, but there are a number of differences.

	Online backup	Cloud archiving
Feature purpose	Data protection from operating system corruption, hardware failures, and loss of separate files.	Cleanup of local storage device and moving data to Acronis Cloud.
Data protection	▪ Overall protection of all data on a computer, especially an operating system. ▪ Protection of frequently used files.	Protection of rarely used and old files, mostly your personal documents, photographs, and so on.
Source data selection	Manual selection.	Manual selection of automatically found files.
Source data handling	The source data is kept in the original location.	The source data is deleted from the original location. This gives you a guarantee that your data will not get into the wrong hands if your hard drive or laptop is stolen.
Data change frequency	The data to back up is changed frequently. Usually a backup has many versions updated from time to time.	The data to archive is changed rarely. The files have few versions.

Copyright © Acronis International GmbH, 2002-2016

6.4 Archiving your data

Data archiving helps you free up your storage space by moving your old or rarely used files to Acronis Cloud or local storage. Refer to What is data archiving (p. 94) for details.

To archive your data:

1. Start Acronis True Image, and then go to the **Archive** section.
2. [Optional step] To learn basics of the data archiving feature, view the Getting Started slides.
3. Do one of the following:
   - To analyze files in your default Windows user folder, usually located at C:\Users\[username], click **Analyze Home folder**.
   - To analyze files in a custom folder, click the down-arrow, click **Select different folder**, and then select the folder to analyze.

   Acronis True Image analyzes files on your computer. Note that this process may take several minutes.
4. In the left area, select a data category. Then, in the right area, select the files and folders that you want to archive.

   When selecting found files, you can sort them, for example, by size or by age (last modified date). To sort the files, click the appropriate column header.
5. Click **Select destination**, and then select Acronis Cloud or a custom local destination for the archived files.
6. [optional step] Click **Options** to set the options for the archive, including **Data center** and **Encryption**. Refer to Data archiving options (p. 96) for details.
7. Click **Archive**.
8. Confirm that you want to move your files to the archive and automatically delete them from your computer.

6.4.1 Data archiving options

Data center

When you archive your files to Acronis Cloud, they are uploaded to one of the Acronis data centers located in different countries. Initially, the data center is defined as the one closest to your location when you create your Acronis account. Afterwards, your archived files are stored in the same data center, by default.

We recommend that you set the data center for an archive manually, when you are in a different country and your default data center is not the closest to your current location. This will significantly increase the data upload rate.

Note: You cannot change the data center after starting the archiving process.

To select a data center:

1. When configuring the first archiving process, click **Options**.
2. Select the country that is closest to your current location.

Copyright © Acronis International GmbH, 2002-2016

Encryption

To protect the archived data from unauthorized access, you can encrypt the archive with industry-standard AES (Advanced Encryption Standard) cryptographic algorithm with a 256-bit long key.

Note: You cannot set or change the archive encryption option for a pre-existing archive.

To encrypt an archive:

1. When configuring the first archiving process, click **Options**.
2. Select the **Encrypt archive by using the AES-256 algorithm** check box.
3. Enter the password for the archive into the corresponding field. We recommend that you use a password longer than seven symbols and containing both letters (in upper and lower cases preferably) and numbers to make it more difficult to guess.

   A password cannot be retrieved. Please memorize the password that you specify for an archive protection.

Acronis True Image asks for the password every time you try to modify the archive. To access the archive, you must specify the correct password.

6.5 Accessing your archived files

When your files are successfully archived, you can access them in:

- **File Explorer**

  Start File Explorer, and then click **Acronis Archive** under **Favorites**.

  You can work with the files as if they were stored on an ordinary hard drive.
- **Acronis Cloud** (applicable to the cloud archive only)

  Open the Acronis Cloud web application in one of the following ways:
  - Start Acronis True Image, click **Archive**, and then click **In your web browser**.
  - Go to https://www.acronis.com/my/online-backup/, log in to your account, and then click **Recover my data now**.

Copyright © Acronis International GmbH, 2002-2016

7 Protecting family data

In this section

What is family data protection? 98
Adding a new device to Online Dashboard 98
Backing up data remotely 99
Recovering data with Online Dashboard 100
Backing up a Facebook account 100
Recovering your Facebook account 101

7.1 What is family data protection?

Family data protection is a unified cross-platform solution that allows you to track and control the protection status of all computers, smartphones, and tablets sharing the same Acronis account. Since users of these devices must be signed in to the same account, usually they are members of the same family. In general, each of them can use this feature, but there is often a family member who is more experienced in technology than the others. So, it's reasonable to make that person responsible for protection of the family data.

To track and control the protection status of your family's devices, use the web-based Online Dashboard, which is accessible from any computer connected to the Internet. With this web application, your family IT administrator can:

- Control the current statuses of all backups and synchronizations on all family devices running Windows, Mac OS X, iOS, and Android.
- Add a new device to the list.
- Manually start any backup on any computer.
- Create new backups of any type (entire machine, file-level, disk-level) on PCs and Macs.
- Change settings of existing backups.
- Recover data from any backup located in Acronis Cloud, including backups from PCs, Macs, and devices running iOS and Android.
- Resolve some product-related issues.

7.2 Adding a new device to Online Dashboard

To use all of the advantages of Online Dashboard, including remote management of your backups, you first need to add your devices to the device list.

To add a new device:

1. Install Acronis True Image on your device.
   - You can download the installation files for Windows and Mac OS X at the Acronis website.
   - To install Acronis True Image on iOS and Android devices, follow the instructions in Installing Acronis True Image for mobile devices (p. 109).
2. Start Acronis True Image and sign in to your Acronis account.

Alternatively, you can add a device via the Online Dashboard interface.

To add a new device via Online Dashboard:

Copyright © Acronis International GmbH, 2002-2016

1. On the device that you want to add, open Online Dashboard at: https://cloud.acronis.com.
2. Sign in with your Acronis account.
3. On the **Resources** tab, click **Add**.
4. Download and install Acronis True Image.
5. Start Acronis True Image and sign in to the same Acronis account.

7.3 Backing up data remotely

With the web-based Online Dashboard, you can configure and run a backup on any computer (PC or Mac) that shares the same Acronis account.

Before backing up, ensure that you have access to a computer:

1. Open Online Dashboard at: https://cloud.acronis.com.
2. Sign in with your Acronis account.
3. On the **Resources** tab, find the computer that you want to back up.
   - If you cannot find the computer, you first need to add it to the list. To do this, install Acronis True Image on that computer, start the application, and then sign in with your Acronis account. Refer to Adding a new device (p. 98) for details.
   - If the computer is offline, make sure that it is turned on and connected to the Internet.

To create the first backup on a computer:

1. Open Online Dashboard, and then find the computer that contains the data that you want to back up.
2. Click **Enable backup**, and then configure settings for the new backup, including:
   - Backup type (entire machine, disk-level, or file-level)
   - Data to back up
   - Backup destination
   - Schedule
   - Retention rules
   - Data encryption
3. When the backup is configured, click **Apply**, and then click **Run now**.

To create a new version of an existing backup:

1. Open Online Dashboard, and then find the computer that contains the data that you want to back up.
2. Click **Back up now**, and then select the backup that you want to update.

To change settings of an existing backup:

1. Open Online Dashboard, and then find the computer that is the source of the backup.
2. Click the gear icon, click **Backup**, and then find the backup that you want to reconfigure.
3. Click the gear icon next to the backup name, and then click one of the following:
   - To change the main settings, click **Edit**.
   - To change additional options, click **Backup options**.
4. Click **Save changes**.

Copyright © Acronis International GmbH, 2002-2016

To create a new backup:

1. Open Online Dashboard, and then find the computer that contains the data that you want to back up.
2. Click the gear icon, and then click **Backup**.
3. Click **Add backup plan**.
   - To create a backup with the predefined settings, click **Apply**. The entire machine will be backed up to Acronis Cloud.
   - To create a backup with custom settings, click **Create new**, change the settings, and then click **Apply**.
4. To start backup, click **Run now**.

7.4 Recovering data with Online Dashboard

The web-based Online Dashboard allows you to recover data from any online backup uploaded from your family devices, including PCs, Macs, smartphones, and tablets.

To recover data from an online backup:

1. Open Online Dashboard at: https://cloud.acronis.com.
2. Sign in with your Acronis account.
3. On the **Resources** tab, find the device that is the source of the data that you want to recover. If the device is offline, make sure that it is turned on and connected to the Internet.
4. Click **Recover**.
5. On the left panel, select the backup version by the backup date and time.
6. On the right panel, select the check boxes next to the files and folders that you want to recover.
7. Click **Download**.

7.5 Backing up a Facebook account

Acronis True Image allows you to protect your entire Facebook account from losing your photos, posts, profile information, and other data and activities. The copy of your account is uploaded to secure Acronis Cloud and is accessible from any device. After uploading the data, you can browse it and recover a specific item or the entire account.

Data that you can back up:

- Profile

  Basic information, including name, email, birth date, gender, website.
- Timeline

  Your posts and posts of other people on your wall.
- Photos and videos

  Your albums, as well as photos and videos you are tagged in.
- Events

  Description of events that you are invited to visit.
- Liked pages

  Links to the pages that you liked, with page names and pictures.

Copyright © Acronis International GmbH, 2002-2016

To back up your Facebook account to Acronis Cloud:

1. Open Online Dashboard by doing one of the following:
   - Follow the link: https://cloud.acronis.com.
   - On the sidebar of Acronis True Image, click **Dashboard**, and then click **Social network backup**.
2. Sign in to your Acronis account.
3. On the sidebar, click **Resources**, click **Add**, and then choose **Facebook**.
4. Click **Back up Facebook**.
5. Log in to your Facebook account.
6. Click **OK** to allow Acronis True Image to access information from your Facebook account. The information will only be used for backup purposes.
7. Configure the backup by selecting the items that you want to back up and setting a schedule for the backup. When done, click **Apply**.
8. To start the backup, click **Run now**.

7.6 Recovering your Facebook account

Acronis True Image allows you to protect your entire Facebook account from losing your photos, posts, profile information, and other data and activities. When you have a cloud backup of your account data, you can browse it and recover a specific item or the entire account.

To browse and recover your Facebook data:

1. Open Online Dashboard by doing one of the following:
   - Follow the link: https://cloud.acronis.com.
   - On the sidebar of Acronis True Image, click **Dashboard**, and then click **Social network backup**.
2. Sign in to your Acronis account.
3. On the sidebar, click **Resources**, and then find the Facebook backup box.
4. Click **Recover**.

   The Online Dashboard opens the list of the backed up items. You can browse them, view their contents, and use search to find a specific item (not available for some data types).

   After selecting an item, you can choose an operation to perform (depending on data type, some operations may be unavailable):
   - **View original**—click to view the selected item on Facebook.
   - **Show content**—click to view the item details or open it in full size.
   - **Download**—click to download the selected file to your device.
   - View an item's comments, likes, tagged users, and detailed information.

Copyright © Acronis International GmbH, 2002-2016

8 Synchronizing data

In this section

About the Sync feature 102
How we ensure security of your data 102
What you can and cannot synchronize 102
Sync icons 103
Sync creation 104
Versions of synchronized files 105
How to clean up your space on Acronis Cloud 105
How to recover a deleted file 107
How to unlink a device from your account 107

8.1 About the Sync feature

The main highlights of the Sync feature:

- An Acronis Cloud subscription is required to use the Sync feature. Refer to Subscription information (p. 25) for details.
- You can have the same data - documents, photos, videos, etc. - on all of your computers. Your data is within easy reach anywhere and anytime. No more emailing files to yourself or carrying an USB drive all the time.
- You can create as many syncs as you need.
- The Acronis Cloud keeps your synced files and versions of those files. This lets you roll back to a previous file version whenever you need it.
- You can also access the Cloud using a web browser, without having to install our application.

8.2 How we ensure security of your data

You may want to be sure that your personal files won't get into the wrong hands. You may be especially concerned about your mobile device, because all of your synced data will be transferred through the Internet.

Let us assure you that your data will be safe. First of all, we use encrypted protocols (SSL, TLS) to transfer all data through both the Internet and LAN . To access the synced data, sign in to your account by providing the e-mail address and password for that account.

Furthermore, we store your data on our servers in encrypted form. Only you have access to your encrypted data.

8.3 What you can and cannot synchronize

You can synchronize data stored in two or more folders. Let's consider where these folders may be located and what data they may contain.

Storage types

A synchronization process may be established between:

- Two or more folders on two or more computers.

Copyright © Acronis International GmbH, 2002-2016

- One or more computers and Acronis Cloud.

  Acronis Cloud always contains the last versions of the synced files. At the same time you cannot select a folder on Acronis Cloud to participate in a sync, such folder is created automatically.
- A mobile device and Acronis Cloud. See details in What is True Image for mobile devices (p. 109).

Within one sync process you may assign only one sync folder on every computer.

You cannot select for synchronization a single file. To synchronize the file, select for synchronization the folder that contains that file.

Data types

You can synchronize the following data:

- Files (your photos, music, videos, documents, etc.), except those listed below

  Only the native FAT32 and NTFS file attributes are synchronized. If the synced folders belong to different file systems, the program synchronizes only the attributes supported by the both file systems.
- Other folders inside the sync folder (that is, sync subfolders) and their content

You cannot synchronize the following data:

- Disks and partitions
- System files and folders
- Hidden files and folders
- Temporary files and folders
- System registry
- Databases
- Data of e-mail programs (including Microsoft Outlook and others)
- Other data that cannot be represented as separate files or folders (for example, contacts from your address book)
- Windows libraries (Documents, Music, etc.)

8.4 Sync icons

While working with syncs you will see special icons. The icons give you the following information:

- Type and current state of your syncs (the icons are shown in the notification area).
- Current state of synced files and folders (the icons are shown in File Explorer).

The notification area

Sync state icons:

Icon	Description
	The synchronization is working in normal mode.
	The synchronization is paused.
	An error occurred during the last synchronization.

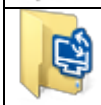
Copyright © Acronis International GmbH, 2002-2016

File Explorer

Sync state icons for files and folders:

Icon	Description
	The file or folder is synchronized.
	The file or folder is being synced at the moment.
	The file or folder has not been synchronized because of an error.

Sync type icons for synced folders:

Icon	Description
	Your default sync.
	Sync with Acronis Cloud.
	Sync between computers synced through a local area network.

8.5 Sync creation

Before you begin a new sync creation, please make sure that the following conditions are met:

- You have an Acronis account and a subscription to the Acronis Cloud service. Refer to Subscription information (p. 25) for details.
- Acronis True Image Home 2012 or later version is installed on every computer.
- If you connect your computers through a local area network, make sure that local connection is established.
- Every computer has connection to the Internet.

To sync files and folders:

1. On the sidebar, click **Sync**.
2. If you are not signed in, enter your Acronis account credentials.
3. If this is your first sync, click **Start**, and then select the folder that you want to synchronize. Acronis True Image will start synchronizing with Acronis Cloud. This is your default sync. Refer to Default sync (p. 105) for details.
4. If this is your second or later sync:
    1. Click the plus sign at the bottom of the sync list.
    2. Decide if you want to include Acronis Cloud in your new sync, and then choose the appropriate sync type.
    3. Select the folder that you want to synchronize, and then click **OK**.
5. To join this sync, start Acronis True Image on your other computers, select this sync in the Sync section, click **Join sync**, and then select the folder that you want to synchronize.

Copyright © Acronis International GmbH, 2002-2016

8.5.1 Default sync

When you start using the Sync feature, your first sync is always the default one.

This sync has the following main features:

- The default sync always syncs with the Acronis Cloud. You cannot unsync the storage.
- It also always stores file versions on the Acronis Cloud.
- The contents of the default sync folder automatically sync with the default sync folders on other computers registered under the same Acronis account.
- It also automatically syncs with your mobile devices that have True Image by Acronis app installed.

Using the default sync is the easiest way to sync your data. If needed, you can also create other syncs.

8.6 Versions of synchronized files

Acronis True Image gives you an opportunity to undo the changes that were made to your files as a result of synchronization. If you find that one of your files contains an undesirable change, you can view previous versions of this file and then choose and rollback to its correct version. See details in Reverting to a previous file version (p. 105).

All versions are stored on the Acronis Cloud which is accessible via the Internet. To use the Acronis Cloud, you must have a subscription to the Acronis Cloud service. If you do not have a subscription, a trial subscription with unlimited storage space will be automatically provided. See details in Subscription information (p. 25).

To delete obsolete versions, run the cleanup operation in the Acronis Cloud web application. See details in How to clean up your space on Acronis Cloud (p. 105).

If you use a trial version of Acronis True Image, all stored versions, including the latest one, are deleted from the Cloud when the trial period expires.

8.6.1 Reverting to a previous file version

If you store sync history on the Acronis Cloud, you can revert the current version of a synchronized file to its previous version. This is useful when you want to undo some undesirable sync operation.

To revert to a previous file version:

1. In the **Sync** section, find the sync box with the needed file. Then click the **Acronis Cloud** link.
2. After the list of sync items opens in your Web browser, select the file which you want to revert to a previous version. Then click the gear icon at the right-hand side. Select **View versions** in the opened menu.
3. Select the version to which you want to rollback. The version's exact date and time will be displayed. Your current version will be reverted to the state it was at that point in time.
4. Click **Recover** to proceed. The selected version will become the latest version on the Cloud. Then, it will be downloaded to the computer that owns the sync.

8.7 How to clean up your space on Acronis Cloud

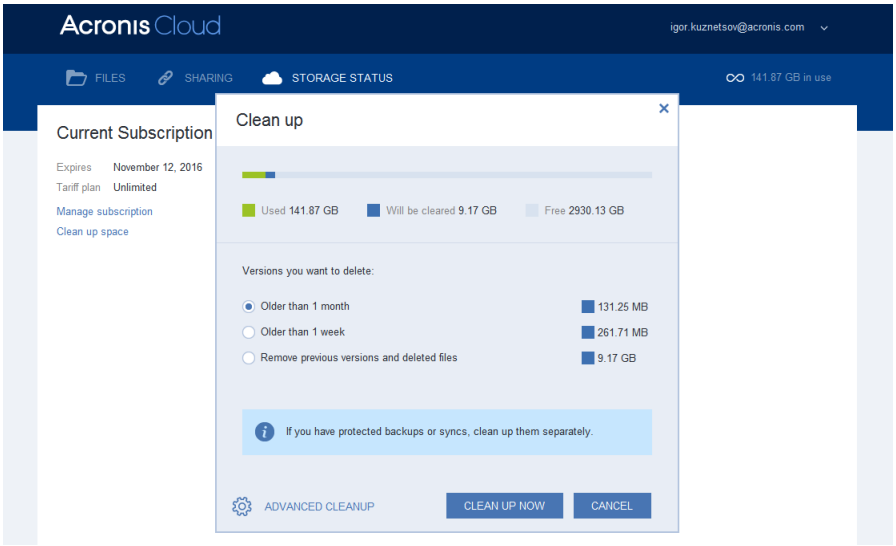
You can clean up your Acronis Cloud space to free it up for fresher data.

Copyright © Acronis International GmbH, 2002-2016

To clean up the Acronis Cloud space:

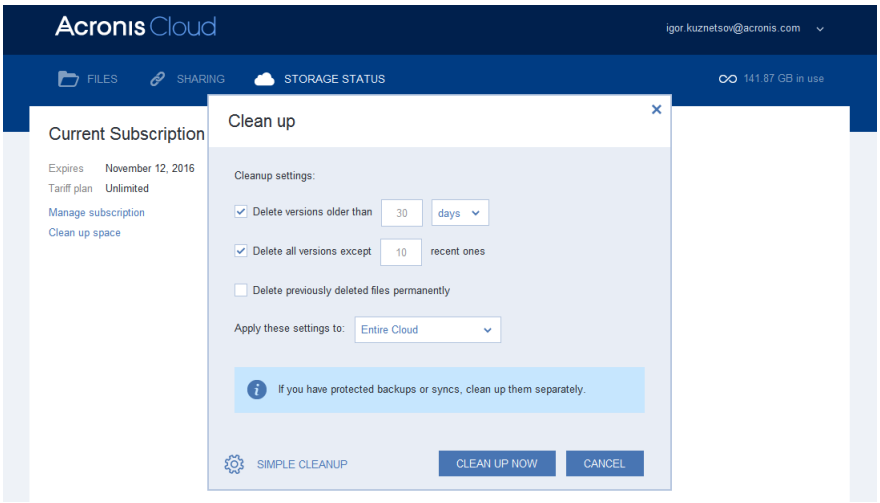
1. On the sidebar, click **Sync**, select the default sync, and then click the **Acronis Cloud** link. The Acronis Cloud web application opens.
2. On the **Storage status** tab, click **Clean up space**.
3. When the appropriate dialog appears, choose which versions you want to delete:
   - All versions.
   - Versions older than one month.
   - Versions older than one week.

   The program shows how much space will be freed up.



Be careful! Deleted versions cannot be restored.

4. Clicking **Advanced cleanup** allows you to select more cleanup rules.



   You can apply the cleanup rules for:
   - individual syncs and online backups
   - all syncs and online backups you have on Acronis Cloud
5. Choose the desired rules and click **Clean up now!.**

One more way to clean up is to delete a sync or online backup which you no longer need. In this case, all version history for the sync or online backup is deleted from Acronis Cloud.

Copyright © Acronis International GmbH, 2002-2016

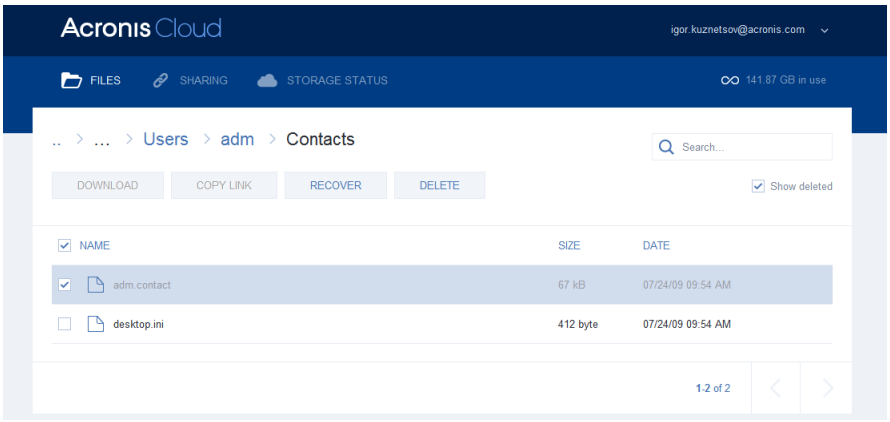
8.8 How to recover a deleted file

Sometimes you may delete a file from a sync by mistake. Then, you need to recover the deleted file. This may be possible for the syncs that keep file versions on Acronis Cloud.

One condition - the deleted file must not be removed during Cloud clean-up.

To recover a deleted file:

1. Start Acronis True Image.
2. On the sidebar, click **Sync**, select the sync that contains the file to recover, and then click the **Acronis Cloud** link.
3. Click the **Files** tab and then select the sync from which you deleted the file.
4. After you select the sync, a list of files and folders appears.
5. Select the **Show deleted** check box and then select the deleted file you want to recover.



6. Click the **Recover** button to recover the deleted file to its folder.

8.9 How to unlink a device from your account

Sometimes you may need to unlink one of your computers or mobile devices from your account. For example, when a computer fails or gets stolen.

To unlink a device:

Go to yourAcronis account page at http://www.acronis.com/my/index.html.

1. Log in to your account.

Copyright © Acronis International GmbH, 2002-2016

2. Click **Synchronization** in the left-hand side of the screen. The **Computers** tab in the Manage synchronization area is displayed by default.

3. Click **Unlink** to the right of the name of the computer you want to unlink.
4. Click **OK** in the confirmation message.

Unlinking the computer:

- Removes it from the Computers list.
- Removes it from all syncs in which the computer participates.
- Blocks the sync participant certificate.

Copyright © Acronis International GmbH, 2002-2016

9 Acronis True Image for mobile devices

Acronis Cloud might be unavailable in your region. For more information, click here: http://kb.acronis.com/content/4541

Acronis True Image for mobile devices allows you to back up your data to Acronis Cloud or to local storage on your computer, and then recover it in case of loss or corruption. Note that backup to the cloud storage requires an Acronis Cloud subscription.

Which devices does the mobile app support?

You can install Acronis True Image on any mobile devices that runs either iOS (iPhone, iPad, iPod) or the Android (mobile phones and tablets) operating systems.

Key features

Acronis True Image for mobile devices allows you to:

- Back up your personal data to Acronis Cloud or local storage on your computer
- Automatically back up new and changed data
- Access cloud backups from all your mobile devices and recover data from these backups

Where can I find these apps?

You can view additional information and download Acronis True Image for mobile devices from the Apple App Store or Google Play:

- Acronis True Image for iOS devices:
  https://itunes.apple.com/us/app/acronis-true-image-cloud/id978342143
- Acronis True Image for Android devices:
  https://play.google.com/store/apps/details?id=com.acronis.acronistrueimage

In this section

Installing Acronis True Image for mobile devices 109
Backing up your mobile device to Acronis Cloud.....110
Backing up your mobile device to a computer 110
Recovering mobile data with your mobile device 111
Recovering data to a new smartphone.....111
Mobile app settings.....112
Local destination of mobile backups.....112

9.1 Installing Acronis True Image for mobile devices

Depending on your mobile device, go to the Apple App Store or Google Play and search for the Acronis True Image app.

For example, to find and install Acronis True Image app for iOS:

1. On your iPhone, open **App Store**.
2. Tap the Search icon.
3. Enter **acronis** in the search field.
4. Select **acronis true image** in the search results to go to the app page.
5. Follow the standard installation procedure.

Copyright © Acronis International GmbH, 2002-2016

The procedure to find and install the Android app is similar.

9.2 Backing up your mobile device to Acronis Cloud

A mobile backup is your guarantee that your data on your mobile device is safe and can be recovered in case of corruption or loss. You can also use the backup to transfer your personal data and settings from your old smartphone to a new one.

To back up your mobile data to Acronis Cloud:

1. Start Acronis True Image.
2. Tap **Back up to Cloud**.
3. Sign in to your Acronis account.
4. Select the data categories that you want to back up.
5. Tap **Back up now**.
6. Allow Acronis True Image to access to your personal data.

When the backup is complete, your data is uploaded to the secure Acronis Cloud. If you want data changes (for example, new photographs) to be backed up automatically, make sure the **Continuous backup** setting is turned on. If this setting is turned off, the new data is backed up only when you tap **Back up**. Refer to Mobile app settings (p. 112) for details.

9.3 Backing up your mobile device to a computer

A mobile backup is your guarantee that your data on your mobile device is safe and can be recovered in case of corruption or loss. You can also use the backup to transfer your personal data and settings from your old smartphone to a new one.

To back up your mobile data to a computer:

1. Make sure that your mobile device and your computer are connected to the same Wi-Fi network.
2. On your computer:
    1. Start Acronis True Image.
    2. On the sidebar, click **Devices**, and then click **Mobile device local backup**.

       A QR code will be displayed. Please do not close this window.
3. On your mobile device:
    1. Start Acronis True Image.
    2. Tap **Back up to PC**.
    3. Tap **I already have it**, or follow the on-screen instructions to install Acronis True Image on your computer.
    4. Tap **Scan QR code**, point your camera at the QR code on the computer screen, and then wait until the mobile device is connected to the computer.
    5. Select the data categories that you want to back up.
    6. Tap **Back up now**.
    7. Allow Acronis True Image to access to your personal data.

When the backup is started, you can track the progress in any application - on the computer or mobile device, but the errors and warning messages are displayed in the mobile app only.

Copyright © Acronis International GmbH, 2002-2016

When the backup is complete, your data is uploaded to your computer. If you want data changes (for example, new photographs) to be backed up automatically, make sure the **Continuous backup** setting is turned on. If this setting is turned off, the new data is backed up only when you tap **Back up**. Refer to Mobile app settings (p. 112) for details.

9.4 Recovering mobile data with your mobile device

With your smartphone or tablet, you can access any mobile backup stored in Acronis Cloud or on your computer. In general, you can open, view, recover, and perform some other operations with a file or data category. Note that because of operating system limitations, some operations can be unavailable for the specific file types.

To access data in a mobile backup:

1. Install and start Acronis True Image.
2. Make sure that you have access to the backup:
   - To access a cloud backup, sign in to your Acronis account, if prompted.
   - To access a local backup, make sure that the mobile device and computer are connected to the same Wi-Fi network.

     Note: To connect to a computer, you need to have Acronis True Image installed on the computer.
3. To open the side menu, slide from the left border of the screen to the right, and then tap **Access and Recovery**.
4. Select the backup that contains the desired file or data category. You can select the backup by name or by the device that contains the desired data. For example, to access data from your current mobile device, select this device from the list.
5. Browse to the desired file or data category.
6. Depending on the data type, the following operations can be done:
   - **Open**
   - **Recover**
   - **Recover all**

9.5 Recovering data to a new smartphone

When you have a mobile backup of your smartphone, you can easily transfer your personal data to another mobile device. For example, this is handy when you buy a new smartphone. Just recover your data from Acronis Cloud, or the local storage on your computer, to your new device.

To recover your data to a new smartphone:

1. Install and start Acronis True Image.
2. Depending on the mobile backup location, do one of the following:
   - If the backup is stored in Acronis Cloud, tap **Back up to Cloud**, and then sign in to your Acronis account.
   - If the backup is stored on your computer, tap **Back up to PC**, make sure that the mobile device and computer are connected to the same Wi-Fi network, and then scan the QR code to connect the mobile device to the computer. Refer to Backing up your mobile device to a computer (p. 110) for details.

   Acronis True Image detects that there are mobile backups in Acronis Cloud or local storage on your computer.

Copyright © Acronis International GmbH, 2002-2016

3. Tap **Recover data**.
4. Select the mobile device to recover your data from, and then tap **Select**. For example, if you want to transfer your data from your old smartphone, select it.
5. Select the data categories that you want to recover, and then tap **Recover**.
6. Allow Acronis True Image access to your personal data.

When the recovery is complete, your data is downloaded to your new device.

9.6 Mobile app settings

To open the **Settings** section, slide from the left border of the screen to the right, and then tap **Settings**. The following settings are available:

- **Continuous backup**

  If this setting is turned on, Acronis True Image automatically detects new data and uploads it to Acronis Cloud.
- **Back up using Wi-Fi only** or **Back up using Wi-Fi and cellular connection**

  You can choose an Internet connection type for the data upload and download. This is useful because sometimes a Wi-Fi connection is cheaper (or free) or more reliable than other connection types.
- **Help**

  Tap this item to open a web-based product help.
- **Send feedback**

  This command allows you to send feedback about Acronis True Image, report a problem, or contact customer support.

9.7 Local destination of mobile backups

When you back up your mobile data to a computer, Acronis True Image stores the backups in the default folder *C:\ProgramData\Acronis Mobile Backup Data\acronis-local-data*. When you change the destination, the *acronis-local-data* folder is moved to the location that you select. During this operation, the current mobile backups are paused and will automatically resume when the operation completes. All new mobile data will be backed up to the new destination.

Note: All mobile backups are always stored in the same folder and cannot be separated.

To change a local destination for mobile backups:

1. On the **Settings** tab, find the **Mobile backup location** option.
2. Click **Change**, then click **Select location**, and then select a new location for the backups. Note, you can select a location only on your internal hard drives.

Copyright © Acronis International GmbH, 2002-2016

10 Disk cloning and migration

This operation copies the entire contents of one disk drive to another disk drive. This may be necessary, for example, when you want to clone your operating system, applications, and data to a new, larger capacity disk. You can do it two ways:

- Use the Clone disk utility (p. 113).
- Back up your old disk drive, and then recover it to the new one (p. 73).

In this section

Disk cloning utility 113
Migrating your system from an HDD to an SSD 118

10.1 Disk cloning utility

The Clone disk utility allows you to clone your hard disk drive by copying the partitions to another hard disk.

Please read before you start:

- When you want to clone your system to a higher-capacity hard disk, we recommend that you install the target (new) drive where you plan to use it and the source drive in another location, e.g. in an external USB enclosure. This is especially important for laptops.

  Warning! Your old and new hard drives must work in the same controller mode (for example, IDE or AHCI). Otherwise, your computer will not start from the new hard drive.

  Warning! If you clone a disk with Windows to an external USB hard drive, you will not be able to boot from it. Windows does not support booting from external USB hard drives. Please clone to internal SSD or HDD instead.

- The Clone disk utility does not support multiboot systems.
- On program screens, damaged partitions are marked with a red circle and a white cross inside in the upper left corner. Before you start cloning, you should check such disks for errors and correct the errors using the appropriate operating system tools.
- We strongly recommend that you create a backup of the entire original disk as a safety precaution. It could be your data saver if something goes wrong with your original hard disk during cloning. For information on how to create such a backup see Backing up partitions and disks (p. 41). After creating the backup, make sure that you validate it.

10.1.1 Clone Disk wizard

Before you start, we recommend that you read general information about Disk cloning utility (p. 113).

We recommend that you clone disks under bootable media. Even when you start cloning in Windows, your computer will restart into the standalone version of Acronis True Image to complete the cloning procedure. In addition, under bootable media you can check if both disks are recognized correctly. This is important to do before you start cloning.

To clone a disk:

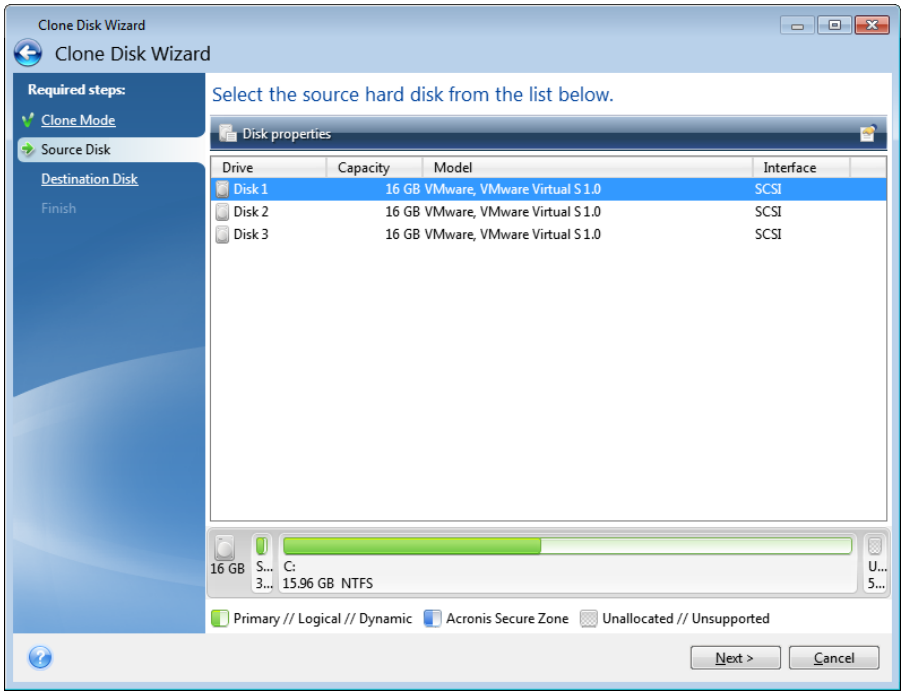
1. On the sidebar, click **Tools**, and then click **Clone disk**.

Copyright © Acronis International GmbH, 2002-2016

2. On the **Clone Mode** step, choose a transfer mode.
   - **Automatic**—Recommended in most cases.
   - **Manual**—Manual mode will provide more data transfer flexibility. Manual mode can be useful if you need to change the disk partition layout.

   If the program finds two disks, one partitioned and another unpartitioned, it will automatically recognize the partitioned disk as the source disk and the unpartitioned disk as the destination disk. In such case, the next steps will be bypassed and you will be taken to the cloning Summary screen.

3. On the **Source Disk** step, select the disk that you want to clone.



   Acronis True Image does not support cloning of dynamic disks.

4. On the **Destination Disk** step, select the destination disk for the cloned data.

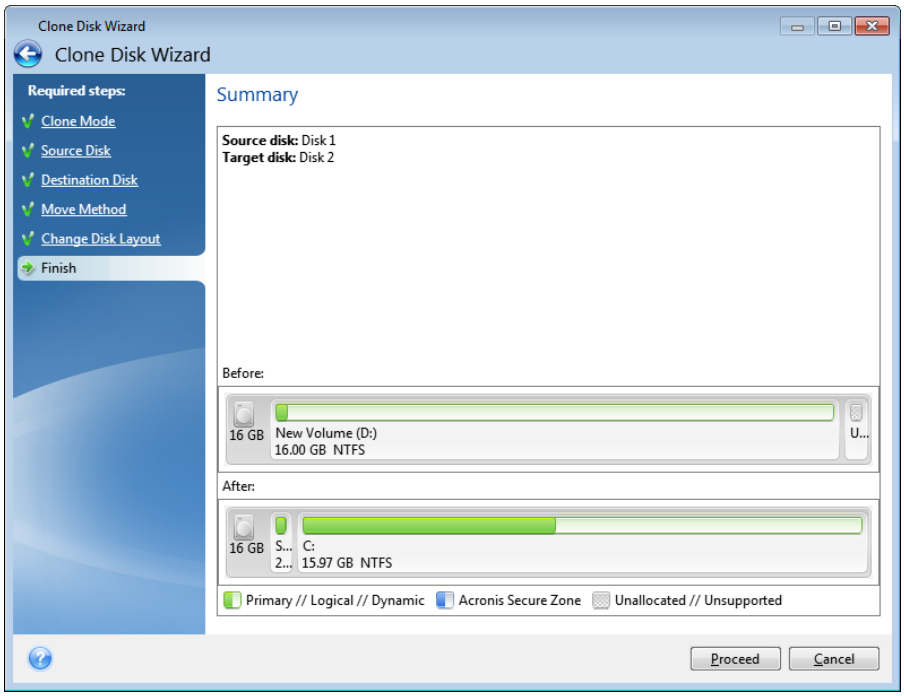
   If the selected destination disk contains partitions, you will need to confirm deletion of the partitions. Note that the real data destruction will be performed only when you click **Proceed** on the last step of the wizard.

   If any disk is unpartitioned, the program will automatically recognize it as the destination and bypass this step.

5. [This step is only available in the manual cloning mode]. On the **Move method** step, choose a data move method.
   - **As is**—a new partition will be created for every old one with the same size and type, file system and label. The unused space will become unallocated.
   - **Proportional**—the new disk space will be proportionally distributed between cloned partitions.
   - **Manual**—you will specify a new size and other parameters yourself.
6. [This step is only available in the manual cloning mode]. On the **Change disk layout** step, you can edit settings of the partitions that will be created on the destination disk. Refer to Manual partitioning (p. 116) for details.
7. [Optional step] On the **What to exclude** step, you can specify files and folders that you do not want to clone. Refer to Excluding items from cloning (p. 117) for details.

Copyright © Acronis International GmbH, 2002-2016

8. On the **Finish** step, ensure that the configured settings suit your needs, and then click **Proceed**.



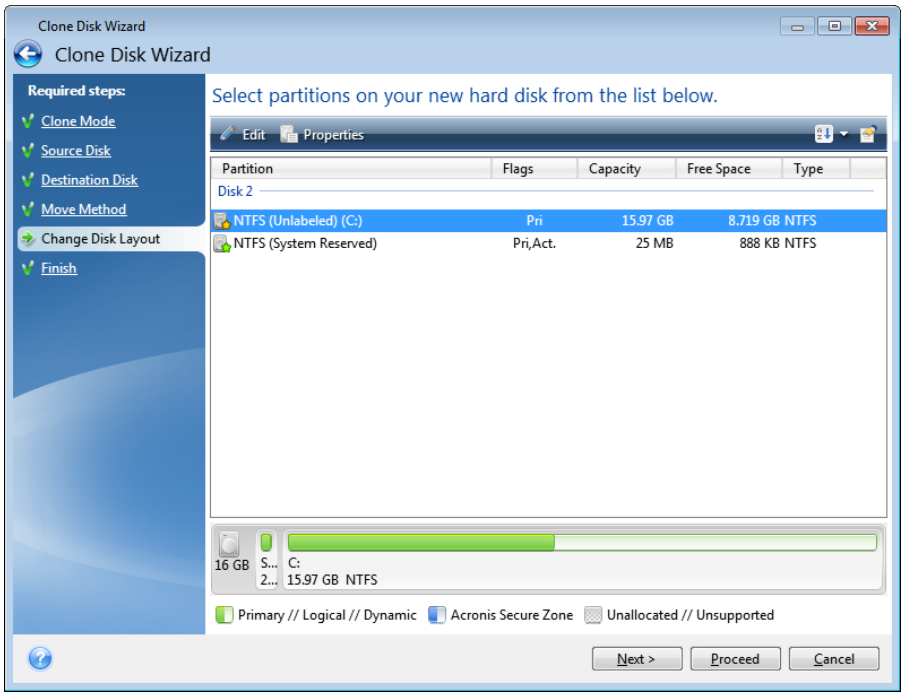
If the cloning operation is stopped for some reason, you will have to configure and start the procedure again. You will not lose your data, because Acronis True Image does not alter the original disk and data stored on it during cloning.

Cloning a disk containing the currently active operating system will require a reboot. In that case, after clicking **Proceed**, you will be asked to confirm the reboot. Canceling the reboot will cancel the entire procedure. By default, Acronis True Image shuts down the computer after the clone process finishes. This enables you to change the position of master/subordinate jumpers and remove one of the hard drives.

Copyright © Acronis International GmbH, 2002-2016

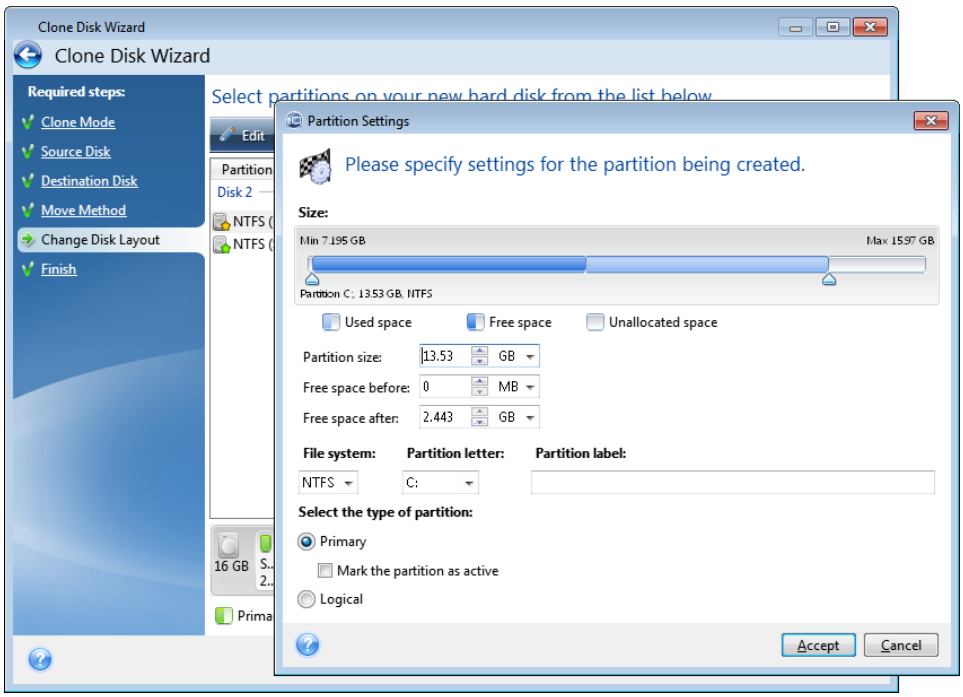
10.1.2 Manual partitioning

The manual transfer method enables you to resize partitions on the new disk. By default, the program resizes them proportionally.



To edit a partition:

1. Select the partition, and then click **Edit**. This will open the Partition Settings window.



2. Specify the following settings for the partition:
   - Size and position
   - File system

Copyright © Acronis International GmbH, 2002-2016

- Partition type (available only for MBR disks)
- Partition letter and label

  Refer to Partition settings (p. 144) for details.

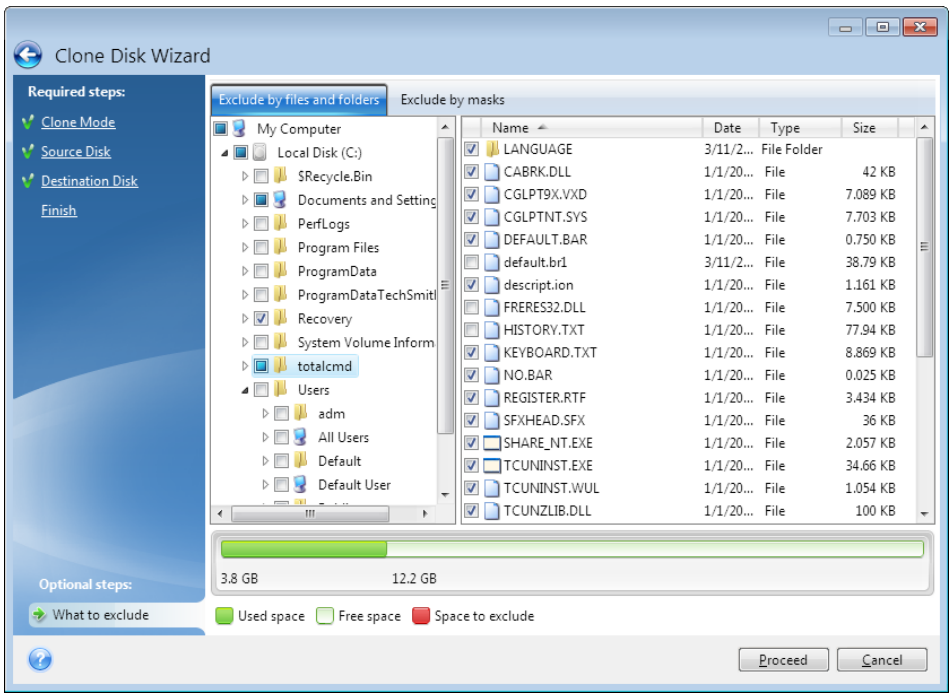
3. Click **Accept**.

Be careful! Clicking any previous wizard step on the sidebar in this window will reset all size and location changes that you've selected, so you will have to specify them again.

10.1.3 Excluding items from cloning

If you do not want to clone specific files from a source disk (for example, when your target disk is smaller than the source one), you can opt to exclude them in the **What to exclude** step.

We do not recommend excluding hidden and system files when cloning your system partition.



You have two ways to exclude files and folders:

- **Exclude by files and folders** - this tab allows you to select specific files and folders from the folder tree.
- **Exclude by masks** - this tab allows you to exclude a group of files by mask or an individual file by name or path.

  To add an exclusion criterion, click **Add**, type a file name, a path or a mask, and then click **OK**. You can add as many files and masks as you like.

Examples of exclusion criteria:

- You can enter explicit file names:
  - *file.ext* - all such files will be excluded from cloning.
  - *C:\file.ext* - the file.ext file on the C: disk will be excluded.
- You can use wildcard characters (* and ?):
  - **.ext* - all files with a .ext extension will be excluded.

Copyright © Acronis International GmbH, 2002-2016

- *??name.ext* - all files with a .ext extension, having six letters in their names (starting with any two symbols (??) and ending with *name*), will be excluded.

- You can enter path to a folder:
  - *C:\my pictures* - *my pictures* folder on the C: disk will be excluded.

You can edit and remove exclusion criteria using the corresponding buttons on the right pane.

10.2 Migrating your system from an HDD to an SSD

First of all, make sure that Acronis True Image detects your new SSD both in Windows and under the Acronis rescue media. If there is a problem, see What to do if Acronis True Image does not recognize your SSD (p. 118).

SSD size

As SSDs usually have less capacity than HDDs, the occupied space on your old hard disk may exceed the size of your SSD. If this is the case, migration is not possible.

To reduce amount of data on your system disk, try the following:

- Move your data files from the old hard disk to another location, such as another hard disk drive, internal or external.
- Create .zip archives of data files (for example, your documents, pictures, audio files, etc.), and then delete the original files.
- Clean up the hard disk using the Windows Disk Cleanup utility.

Note that for stable operation, Windows needs to have several GB of free space on the system partition.

Which migration method to choose

If your system disk consists of a single partition (not counting the hidden System Reserved partition), you can try to migrate to the SSD using the Clone tool. For more information see Cloning a hard disk (p. 113).

However, we recommend to use the backup and recovery method in most cases. This method provides more flexibility and control over migration. See Migrating to an SSD using the backup and recovery method (p. 119).

10.2.1 What to do if Acronis True Image does not recognize your SSD

Sometimes Acronis True Image may not recognize an SSD.

In such a case, check whether the SSD is recognized in BIOS.

If the BIOS of your computer does not show the SSD, verify that the power and data cables are properly connected. You may also try to update the BIOS and SATA drivers. If these suggestions do not help, contact the Support of your SSD manufacturer.

If the BIOS of your computer does show the SSD, you can try the following procedure:

Depending on your operating system, type **cmd** in the Search field or in the Run field, and then press **Enter**.

 Copyright © Acronis International GmbH, 2002-2016

At the command line prompt type:

`diskpart`

`list disk` The screen will show the disks connected to your computer. Find out the disk number for your SSD. Use its size as the reference.

`select disk N` Here N is the disk number of your SSD.

`clean` This operation removes all information from the SSD and overwrites the MBR with the default one.

`exit`

`exit`

Start Acronis True Image and check whether it detects the SSD. If it detects the SSD, use the Add new disk tool to create a single partition on the disk occupying the entire disk space. When creating a partition, check that the free space before partition is 1 MB. For more information, see Adding a new hard disk (p. 141).

The next step is to check whether your Acronis bootable rescue media recognizes the SSD.

1. Boot from the rescue media.
2. Select **Tools & Utilities -> Add New Disk** in the main menu and the **Disk selection** screen will show the information about all hard disks in your system. Use this for checking whether the SSD is detected in the recovery environment.
3. If the screen shows your SSD, just click **Cancel**.

If the rescue media does not recognize the SSD and the SSD controller mode is AHCI, you can try to change the mode to IDE (or ATA in some BIOS brands) and see whether this solves the problem.

Attention! Do not start Windows after changing the mode; it may result in serious system problems. You must return the mode to AHCI before starting Windows.

If after changing the mode the rescue media detects the SSD, you may use the following procedure for recovery or cloning under rescue media:

1. Shut down the computer.
2. Boot to BIOS, change the mode from AHCI to IDE (or ATA in some BIOS brands).
3. Boot from Acronis rescue media.
4. Recover or clone the disk.
5. Boot to BIOS and change IDE back to AHCI.
6. Start Windows.

What to do if the above suggestions do not help

You can try to create a WinPE-based rescue media. This may provide the necessary drivers. For more information, see Creating WinPE-based rescue media.

10.2.2 Migrating to SSD using the backup and recovery method

You can use the following procedure for all supported operating systems. First, let's consider a simple case: your system disk consists of a single partition. Note that for Windows 7 and later, the system disk may have a hidden System Reserved partition.

Copyright © Acronis International GmbH, 2002-2016

We recommend that you migrate your system to an empty SSD that does not contain partitions (the disk space is unallocated). Note that if your SSD is new and has never been used before, it does not contain partitions.

To migrate your system to an SSD:

1. Start Acronis True Image.
2. Create Acronis rescue media, if you do not have it yet. To do this, in the **Tools** section, click **Create bootable media** and follow the instructions on the screen.
3. Back up your entire system drive (in the disk backup mode) to a hard disk other than your system hard disk and the SSD.
4. Switch off the computer and remove your system hard disk.
5. Mount the SSD into the slot where the hard disk was.

   For some SSD brands you may need to insert the SSD into a PCI Express slot.
6. Boot from your Acronis rescue media.
7. Validate the backup to make sure that it can be used for recovery. To do this, click **Recovery** on the left pane and select the backup. Right-click, select **Validate Archive** in the shortcut menu and then click **Proceed**.
8. After the validation finishes, right-click the backup and select **Recover** in the shortcut menu.
9. Choose **Recover whole disks and partitions** at the Recovery method step and then click **Next**.
10. Select the system disk at the What to recover step.
11. Click **New location** and then select the SSD as the new location for your system disk, then click **Accept**.
12. At the next step click **Proceed** to start recovery.
13. After the recovery is complete, exit the standalone version of Acronis True Image.
14. Try to boot from the SSD and then make sure that Windows and applications work correctly.

If your system hard disk also contains a hidden recovery or diagnostic partition, as is quite often the case with notebooks, the procedure will differ. You will usually need to resize the partitions manually during recovery to the SSD. For instructions see Recovering a disk with a hidden partition (p. 73).

 Copyright © Acronis International GmbH, 2002-2016

11 Tools

Acronis Tools and utilities include protection tools, mounting tools, clone disk utility, security and privacy utilities, and disk management utilities.

Protection tools

- **Acronis Universal Restore media**

  If you recover your image on a computer with a dissimilar hardware configuration, the program may not be able to find some of device drivers in the default folders, especially when the target hardware has a specific mass storage controller.

  This tool can be found in the **Tools** tab in Acronis True Image or downloaded from your Acronis account. See details at: https://kb.acronis.com/ati2017/aur.

- **Acronis Startup Recovery Manager** (p. 131)

  Allows you to start Acronis True Image without loading the operating system by pressing F11 at boot time before the operating system starts.

- **Rescue Media Builder** (p. 122)

  Allows you to create a bootable rescue media with Acronis products (or their specified components) installed on your computer.

- **Acronis Secure Zone** (p. 137)

  Allows you to store your backups in a special safe partition on your disk.

- **Try&Decide** (p. 132)

  Try any unsafe operation in the Try mode and then decide whether to apply or discard it.

Disk cloning

- **Clone disk** (p. 113)

  Use Clone disk wizard if you need to clone your hard disk drive by copying the partitions to another hard disk.

Security and privacy

- **Acronis DriveCleanser** (p. 145)

  Acronis DriveCleanser utility provides for secure destruction of data on your hard disk.

- **System Clean-up** (p. 149)

  With the System Clean-up utility, you can clean up components (folders, files, registry sections, etc.), related to general system tasks. These Windows components retain evidence of user PC activity, so they too should be thoroughly wiped to maintain confidentiality.

Disk management

- **Add new disk** (p. 141)

  Add new disk wizard helps you to add a new hard disk drive to your computer. You will be able to prepare the new hard disk drive by creating and formatting new partitions on this hard disk.

Image mounting

- **Mount image** (p. 156)

  With this tool you can explore a previously created image. You will be able to assign temporary drive letters to the partition images and easily access these images as ordinary, logical drives.

- **Unmount image** (p. 157)

Copyright © Acronis International GmbH, 2002-2016

With this tool you can unmount the temporary logical drives you have created to explore an image.

11.1 Creating bootable rescue media

You can run Acronis True Image from a bootable media on a bare-metal system or a crashed computer that cannot boot. You can even back up disks on a non-Windows computer, copying all its data into the backup by imaging the disk in the sector-by-sector mode. To do so, you need bootable media that has a copy of the standalone Acronis True Image version installed on it.

How you can obtain bootable media:

- Use the installation CD of the boxed product.
- Make a media bootable with Acronis Media Builder (p. 122):
  - Blank CD
  - Blank DVD
  - USB flash drive

    Note: The data it may contain will not be modified.
  - Create an .iso image file to burn it afterwards onto a CD or DVD.
  - Create WinPE-based media with Acronis plug-in.

11.1.1 Acronis Media Builder

Acronis Media Builder allows you to make a USB flash drive or a blank CD/DVD bootable. In case Windows cannot start, use the bootable media to run a standalone version of Acronis True Image and recover your computer.

You can create several types of bootable media:

- **Acronis bootable rescue media**

  This type is recommended for most users.
- **WinPE-based media with Acronis plug-in**

  Running Acronis True Image in the preinstallation environment may provide better compatibility with your computer's hardware because the preinstallation environment uses Windows drivers.

  We recommend that you create this type of media, when Acronis bootable rescue media did not help you boot your computer.

  To use this option, you need one the following components to be installed:
  - Windows Automated Installation Kit (AIK).

    This component is required for creating WinPE 3.0.
  - Windows Assessment and Deployment Kit (ADK).

    This component is required for creating WinPE 4.0, WinPE 5.0, and WinPE 10.0.

Notes

- We recommend that you create a new bootable media after each Acronis True Image update.
- If you use non-optical media, the media must have FAT16 or FAT32 file system.
- Acronis Media Builder supports only x64 WinPE 3.0, WinPE 4.0, WinPE 5.0, and WinPE 10.0.
- Your computer must have:
  - For WinPE 3.0—at least 256 MB RAM

Copyright © Acronis International GmbH, 2002-2016

  - For WinPE 4.0—at least 512 MB RAM
  - For WinPE 5.0—at least 1 GB RAM
  - For WinPE 10.0—at least 512 MB RAM
- If Acronis Media Builder does not recognize your USB flash drive, you can try using the procedure described in an Acronis Knowledge Base article at http://kb.acronis.com/content/1526.
- When booting from the Rescue Media, you cannot perform backups to disks or partitions with Ext2/Ext3/Ext4, ReiserFS, and Linux SWAP file systems.
- When booting from the rescue media and using a standalone version of Acronis True Image you cannot recover files and folders encrypted with use of the encryption available in Windows XP and later operating systems. For more information, see File-level security settings for backup (p. 60). On the other hand, backups encrypted using the Acronis True Image encryption feature can be recovered.

11.1.1.1 Creating bootable media

To create bootable media:

1. Plug in a USB flash drive, or insert a blank CD or DVD.
2. Start Acronis True Image.
3. In the **Tools** section, click **Rescue Media Builder**.
4. Choose a media type that you want to create. Refer to Acronis Media Builder (p. 122) for details.
5. Select a destination for the media:
   - **CD**
   - **DVD**
   - **USB flash drive**

     If your drive has an unsupported file system, Acronis True Image will suggest formatting it to FAT file system.

     Warning! *Formatting permanently erases all data on a disk.*
   - **ISO image file**

     You will need to specify the .iso file name and the destination folder.

     When the .iso file is created, you can burn it onto a CD or DVD. For example, in Windows 7 and later, you can do this using a built-in burning tool. In File Explorer, double-click the created ISO image file, and then click **Burn**.
   - **WIM image file** (available only for WinPE-based media)

     Acronis True Image adds the Acronis plug-in to the .wim file from Windows AIK or Windows ADK. You will need to specify a name for the new .wim file and the destination folder.

     To create a bootable media by using a .wim file, you first need to convert it to an .iso file. Refer to Creating an .iso file from a .wim file (p. 126) for details.
6. Click **Proceed**.

11.1.1.2 Bootable media startup parameters

Here, you can set bootable media startup parameters in order to configure rescue media boot options for better compatibility with different hardware. Several options are available (nousb, nomouse, noapic, etc.). These parameters are provided for advanced users. If you encounter any hardware compatibility problems while testing boot from the rescue media, it may be best to contact Acronis Technical Support.

Copyright © Acronis International GmbH, 2002-2016

To add startup parameters:

- Enter a command into the **Parameters** field. You can type several commands, separated by spaces.
- Click **Next** to continue.

Additional parameters that can be applied prior to booting Linux kernel

Description

The following parameters can be used to load Linux kernel in a special mode:

- **acpi=off**

Disables ACPI and may help with a particular hardware configuration.

- **noapic**

Disables APIC (Advanced Programmable Interrupt Controller) and may help with a particular hardware configuration.

- **nousb**

Disables loading of USB modules.

- **nousb2**

Disables USB 2.0 support. USB 1.1 devices still work with this option. This option allows using some USB drives in USB 1.1 mode, if they do not work in USB 2.0 mode.

- **quiet**

This parameter is enabled by default and the startup messages are not displayed. Deleting it will result in the startup messages being displayed as the Linux kernel is loaded and the command shell being offered prior to running the Acronis program.

- **nodma**

Disables DMA for all IDE disk drives. Prevents kernel from freezing on some hardware.

- **nofw**

Disables FireWire (IEEE1394) support.

- **nopcmcia**

Disables PCMCIA hardware detection.

- **nomouse**

Disables mouse support.

- **[module name]=off**

Disables the module (e.g. **sata_sis=off**).

- **pci=bios**

Forces to use PCI BIOS, and not to access the hardware device directly. For instance, this parameter may be used if the machine has a non-standard PCI host bridge.

- **pci=nobios**

 Copyright © Acronis International GmbH, 2002-2016

Disallows use of PCI BIOS; only direct hardware access methods are allowed. For instance, this parameter may be used if you experience crashes upon boot-up, probably caused by the BIOS.

- **pci=biosirq**

Uses PCI BIOS calls to get the interrupt routing table. These calls are known to be buggy on several machines and they hang the machine when used, but on other computers it is the only way to get the interrupt routing table. Try this option, if the kernel is unable to allocate IRQs or discover secondary PCI buses on your motherboard.

- **vga=ask**

Gets the list of the video modes available for your video card and allows selecting a video mode most suitable for the video card and monitor. Try this option, if the automatically selected video mode is unsuitable for your hardware.

11.1.1.3 Creating a custom WinPE ISO with your drivers

Sometimes a basic WinPE disk with Acronis Plug-in does not have drivers for your specific hardware, for example, for storage device controllers. You can add such drivers to the basic WinPE image (WIM) before creating an ISO file with Acronis Plug-in.

Attention! You can only add drivers which have the .inf filename extension.

The following procedure is based on an MSDN article that can be found at http://technet.microsoft.com/en-us/library/dd799244(WS.10).aspx

To create a custom Windows PE image, proceed as follows:

1. If you don't have the .wim file with the Acronis plug-in, start **Rescue Media Builder** and create it by choosing **WIM file** as a destination for the WinPE-based media. Refer to Creating bootable media (p. 123) for details.
2. Depending on your version of Windows AIK or Windows ADK, do one of the following:
   - In the **Start** menu, click **Microsoft Windows AIK**, right-click **Windows PE Tools Command Prompt**, and then select **Run as administrator**.
   - In the **Start** menu, click **Microsoft Windows AIK**, right-click **Deployment Tools Command Prompt**, and then select **Run as administrator**.
   - In the **Start** menu, click **Windows Kits**, click **Windows ADK**, right-click **Deployment and Imaging Tools Environment**, and then select **Run as administrator**.
3. Run the Copype.cmd script to create a folder with Windows PE files. For example, from a command prompt, type:
   ```
   copype amd64 C:\winpe_x64
   ```
4. Copy your .wim file, for example, to folder C:\winpe_x64\. By default, this file is named AcronisBootablePEMedia.wim.
5. Mount the base image to a local directory by using the DISM tool. To do this, type:
   ```
   Dism /Mount-Wim /WimFile:C:\winpe_x64\AcronisBootablePEMedia.wim /index:1
   /MountDir:C:\winpe_x64\mount
   ```
6. Add your hardware driver, by using the DISM command with the Add-Driver option. For example, to add the Mydriver.inf driver located in folder C:\drivers\, type:
   ```
   Dism /image:C:\winpe_x64\mount /Add-Driver /driver:C:\drivers\mydriver.inf
   ```
7. Repeat the previous step for each driver that you need to add.
8. Commit the changes by using the DISM command:

Copyright © Acronis International GmbH, 2002-2016

```
Dism /Unmount-Wim /MountDir:C:\winpe_x64\mount /Commit
```

9. Create a PE image (.iso file) from the resulting .wim file. Refer to Creating an .iso file from a .wim file for details.

11.1.1.4 Creating an .iso file from a .wim file

To create a bootable media by using a .wim file, you need to convert it to an .iso file first.

To create a PE image (.iso file) from the resulting .wim file:

1. Depending on your version of Windows AIK or Windows ADK, do one of the following:
   - In the **Start** menu, click **Microsoft Windows AIK**, right-click **Windows PE Tools Command Prompt**, and then select **Run as administrator**.
   - In the **Start** menu, click **Microsoft Windows AIK**, right-click **Deployment Tools Command Prompt**, and then select **Run as administrator**.
   - In the **Start** menu, click **Windows Kits**, click **Windows ADK**, right-click **Deployment and Imaging Tools Environment**, and then select **Run as administrator**.
2. Run the Copype.cmd script to create a folder with Windows PE files. For example, from a command prompt, type:
   ```
   copype amd64 C:\winpe_x64
   ```
3. Replace the default boot.wim file in your Windows PE folder with the newly created .wim file (for example, AcronisBootablePEMedia.wim). If the AcronisBootablePEMedia.wim file is located on c:\, then:

   For WinPE 3.0, type:
   ```
   copy c:\AcronisBootablePEMedia.wim c:\winpe_x64\ISO\sources\boot.wim
   ```
   For WinPE 4.0, WinPE 5.0 or WinPE 10.0, type:
   ```
   copy "c:\AcronisBootablePEMedia.wim" c:\winpe_x64\media\sources\boot.wim
   ```
4. Use the **Oscdimg** tool. To create an .iso file, type:
   ```
   oscdimg -n –bc:\winpe_x64\etfsboot.com c:\winpe_x64\ISO
   c:\winpe_x64\winpe_x64.iso
   ```
   Alternatively, to make the media bootable on both BIOS and UEFI computers, type:
   ```
   oscdimg -m -o -u2 -udfver102
   -bootdata:2#p0,e,bc:\winpe_x64\etfsboot.com#pEF,e,bc:\winpe_x64\efisys.bin
   c:\winpe_x64\ISO c:\winpe_x64\winpe_x64.iso
   ```
5. Burn the .iso file to a CD by using a third-party tool, and you will have a bootable Windows PE disc with Acronis True Image.

11.1.2 Making sure that your rescue media can be used when needed

To maximize the chances of your computer's recovery, you must test that your computer can boot from the rescue media. In addition, you must check that the rescue media recognizes all your computer's devices, such as the hard drives, the mouse, the keyboard, and network adapter.

If you purchased a boxed version of the product that has a bootable CD and you did not update Acronis True Image, you can test this CD. Otherwise, please create a new bootable media. Refer to Creating bootable media (p. 123) for details.

Copyright © Acronis International GmbH, 2002-2016

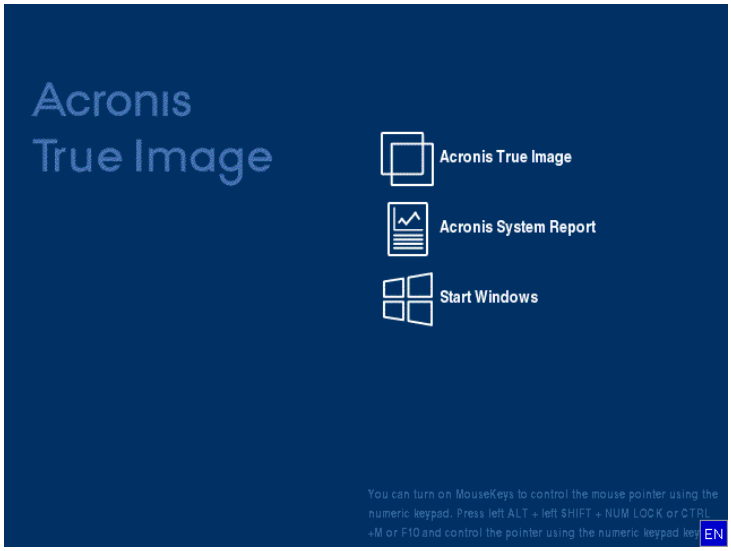
To test the rescue media

If you use external drives for storing your backups, you must attach the drives before booting from the rescue CD. Otherwise, the program might not detect them.

1. Configure your computer to enable booting from the rescue media. Then, make your rescue media device (CD-ROM/DVD-ROM drive or USB stick) the first boot device. See Arranging boot order in BIOS.
2. If you have a rescue CD, press any key to start booting from the CD, when you see the prompt "Press any key to boot from CD". If you do not press a key within five seconds, you will need to restart the computer.
3. After the boot menu appears, choose **Acronis True Image**.

   If your wireless mouse does not work, try to replace it with a wired one. The same recommendation applies to the keyboard.

   If you do not have a spare mouse or keyboard, contact Acronis Support. They will build a custom rescue CD that will have drivers for your models of the mouse and keyboard. Please be aware that finding the appropriate drivers and making the custom rescue CD may take some time. Furthermore, this may be impossible for some models.


Acronis
True Image
Acronis True Image
Acronis System Report
Start Windows
You can turn on MouseKeys to control the mouse pointer using the
numeric keypad. Press left ALT + left SHIFT + NUM LOCK or CTRL
+M or F10 and control the pointer using the numeric keypad ke
EN

4. When the program starts, we recommend you try recovering some files from your backup. A test recovery allows you to make sure that your rescue CD can be used for recovery. In addition, you will check that the program detects all the hard drives you have in your system.

   If you have a spare hard drive, we strongly recommend that you try a test recovery of your system partition to this hard drive.

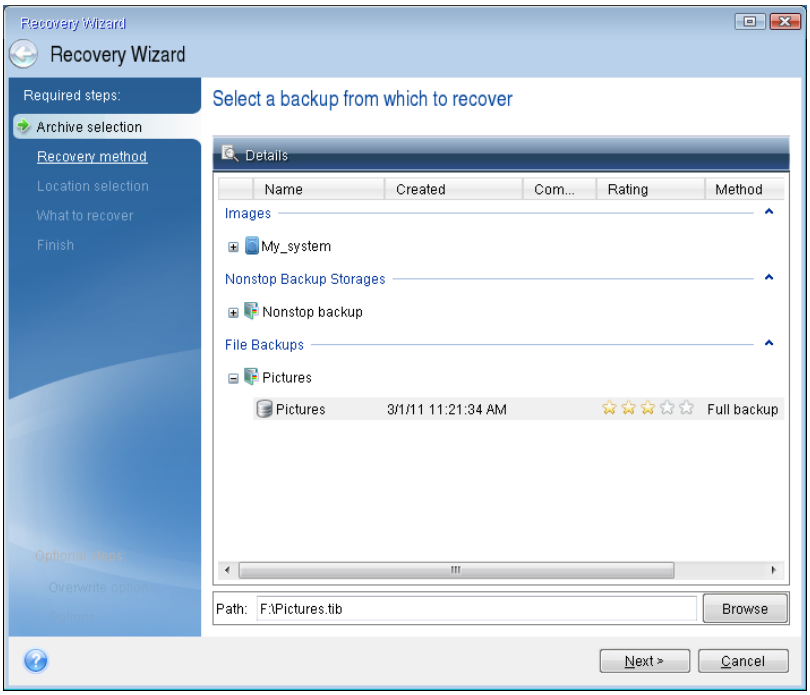
How to test recovery, as well as check the drives and network adapter

1. If you have file backups, start Recovery Wizard by clicking **Recovery** -> **File Recovery** on the toolbar.

   *If you have only disk and partition backup, Recovery Wizard also starts and the recovery procedure is similar. In such a case, you need to select **Recover chosen files and folders** at the **Recovery Method** step.*

Copyright © Acronis International GmbH, 2002-2016

2. Select a backup at the **Archive location** step and then click **Next**.

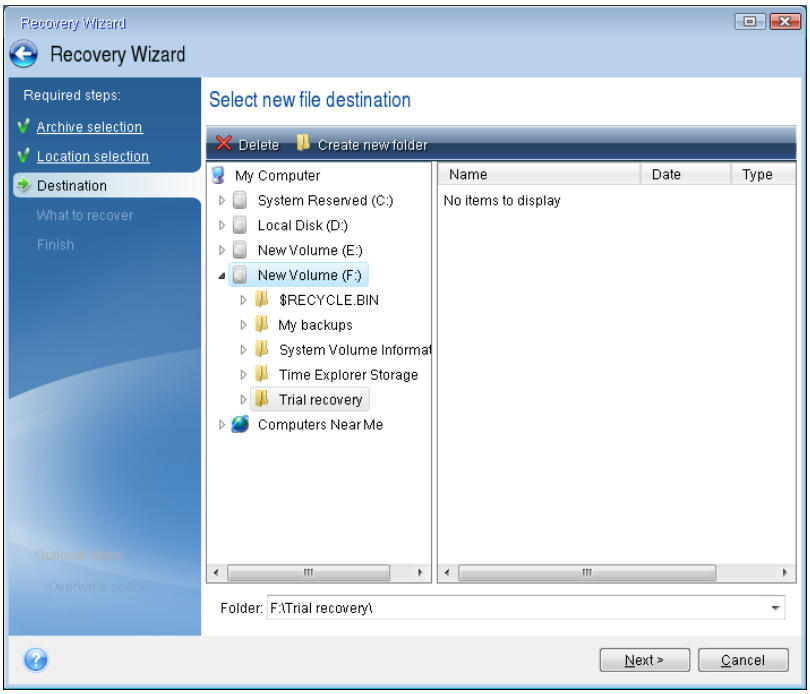


3. When recovering files with the rescue CD you are able to select only a new location for the files to be recovered. Therefore just click **Next** at the **Location selection** step.
4. After the **Destination** window opens, check that all your drives are shown under **My Computer**.

If you store your backups on the network, you should also check that you can access the network.

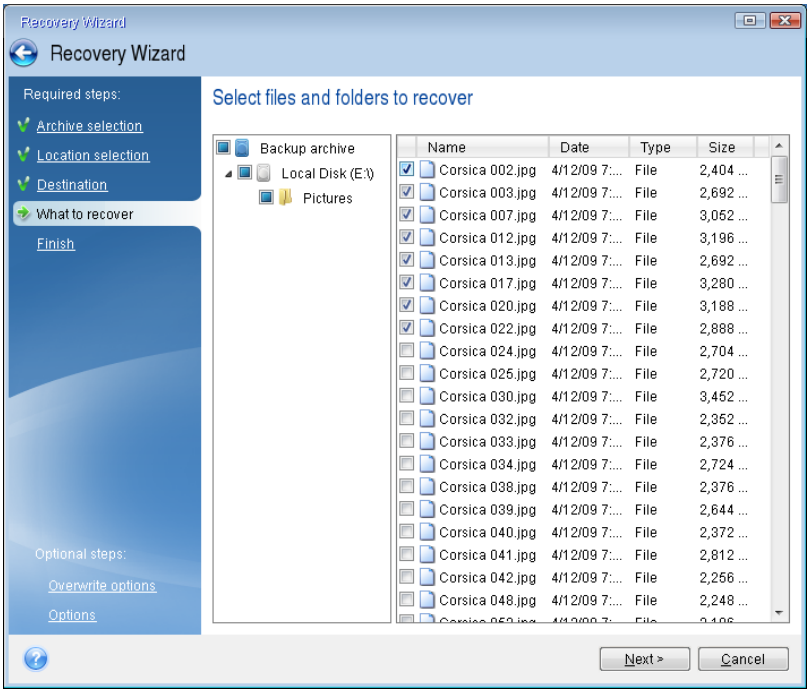
*If no computers are visible on the network, but the **Computers Near Me** icon is found under **My Computer**, specify network settings manually. To do this, open the window available at **Tools & Utilities** → **Options** → **Network adapters**.*

*If the **Computers Near Me** icon is not available under **My Computer**, there may be problems either with your network card or with the card driver provided with Acronis True Image.*



Copyright © Acronis International GmbH, 2002-2016

5. Select the destination for the files and then click Next.
6. Select several files for recovery by selecting their check boxes and then click **Next**.


Recovery Wizard
Recovery Wizard
Required steps:
Archive selection
Location selection
Destination
What to recover
Finish
Optional steps:
Overwrite options
Options
Select files and folders to recover
Backup archive
Local Disk (E:\)
Pictures
Name
Date
Type
Size
Corsica 002.jpg 4/12/09 7:... File 2,404 ...
Corsica 003.jpg 4/12/09 7:... File 2,692 ...
Corsica 007.jpg 4/12/09 7:... File 3,052 ...
Corsica 012.jpg 4/12/09 7:... File 3,196 ...
Corsica 013.jpg 4/12/09 7:... File 2,692 ...
Corsica 017.jpg 4/12/09 7:... File 3,280 ...
Corsica 020.jpg 4/12/09 7:... File 3,188 ...
Corsica 022.jpg 4/12/09 7:... File 2,888 ...
Corsica 024.jpg 4/12/09 7:... File 2,704 ...
Corsica 025.jpg 4/12/09 7:... File 2,720 ...
Corsica 030.jpg 4/12/09 7:... File 3,452 ...
Corsica 032.jpg 4/12/09 7:... File 2,352 ...
Corsica 033.jpg 4/12/09 7:... File 2,376 ...
Corsica 034.jpg 4/12/09 7:... File 2,724 ...
Corsica 038.jpg 4/12/09 7:... File 2,376 ...
Corsica 039.jpg 4/12/09 7:... File 2,644 ...
Corsica 040.jpg 4/12/09 7:... File 2,372 ...
Corsica 041.jpg 4/12/09 7:... File 2,812 ...
Corsica 042.jpg 4/12/09 7:... File 2,256 ...
Corsica 048.jpg 4/12/09 7:... File 2,248 ...
Next >
Cancel

7. Click **Proceed** on the Summary window to start recovery.
8. After the recovery finishes, exit the standalone Acronis True Image.

Now you can be reasonably sure that your rescue CD will help you when needed.

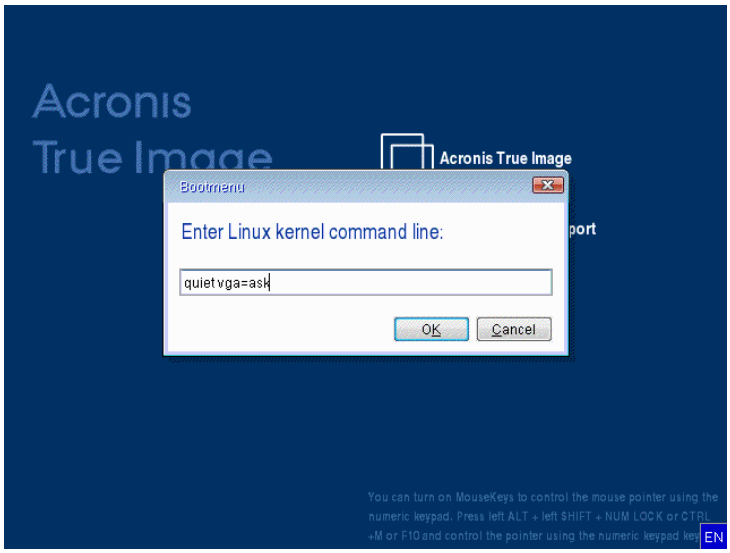
11.1.2.1 Selecting video mode when booting from the rescue media

When booting from the rescue media the optimal video mode is selected automatically depending on the specifications of your video card and monitor. However, sometimes the program can select the wrong video mode, which is unsuitable for your hardware. In such case you can select a suitable video mode as follows:

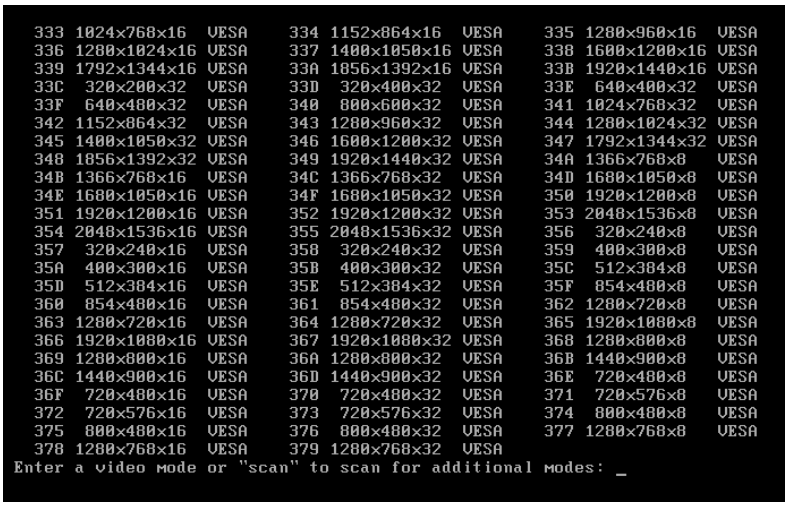
1. Start booting from the rescue media. When the boot menu appears, hover the mouse over **Acronis True Image** item and press the F11 key.

Copyright © Acronis International GmbH, 2002-2016

2. When the command line appears, type "vga=ask" (without quotes) and click **OK**.


Acronis
True Image
Acronis True Image
Bootmenu
Enter Linux kernel command line:
quiet vga=ask
OK
Cancel
port
You can turn on MouseKeys to control the mouse pointer using the
numeric keypad. Press left ALT + left SHIFT + NUM LOCK or CTRL
+M or F10 and control the pointer using the numeric keypad
EN

3. Select **Acronis True Image** in the boot menu to continue booting from the rescue media. To see the available video modes, press the Enter key when the appropriate message appears.
4. Choose a video mode you think best suitable for your monitor and type its number in the command line. For instance, typing 338 selects video mode 1600x1200x16 (see the below figure).



5. Wait until Acronis True Image starts and make sure that the quality of the Welcome screen display on your monitor suits you.

To test another video mode, close Acronis True Image and repeat the above procedure.

After you find the optimal video mode for your hardware, you can create a new bootable rescue media that will automatically select that video mode.

To do this, start Acronis Media Builder, select the required media components, and type the mode number with the "0x" prefix (0x338 in our instance) in the command line at the "Bootable media startup parameters" step, then create the media as usual.

Copyright © Acronis International GmbH, 2002-2016

11.2 Acronis Startup Recovery Manager

How it works

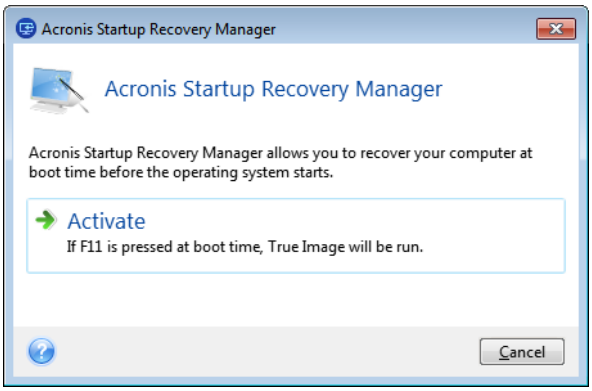
The Acronis Startup Recovery Manager lets you start Acronis True Image without loading the operating system. With this feature, you can use Acronis True Image by itself to recover damaged partitions, even if the operating system won't boot. Unlike booting from Acronis removable media, you will not need a separate media or network connection to start Acronis True Image.

Note: Acronis Startup Recovery Manager cannot be used on tablets running Windows.

How to activate

To activate Acronis Startup Recovery Manager:

1. Start Acronis True Image.
2. In the **Tools** section, click **More tools**, and then double-click **Activate Acronis Startup Recovery Manager**.
3. In the opened window, click **Activate**.


Acronis Startup Recovery Manager
Acronis Startup Recovery Manager
Acronis Startup Recovery Manager allows you to recover your computer at boot time before the operating system starts.
Activate
If F11 is pressed at boot time, True Image will be run.
Cancel

How to use

If a failure occurs, turn on the computer and press F11 when you see the "Press F11 for Acronis Startup Recovery Manager" message. This will start a standalone version of Acronis True Image that differs only slightly from the complete version.

Additional information

Disk letters in standalone Acronis True Image might sometimes differ from the way Windows identifies drives. For example, the D: disk identified in the standalone Acronis True Image might correspond to the E: disk in Windows. The disk labels and information on partition sizes, file systems, drive capacities, their manufacturers, and model numbers can help in correctly identifying the disks and partitions.

You won't be able to use the previously activated Acronis Startup Recovery Manager if the Try&Decide is turned on. Rebooting the computer in the Try mode will allow you to use Acronis Startup Recovery Manager again.

Does Acronis Startup Recovery Manager affect other loaders?

When Acronis Startup Recovery Manager is activated, it overwrites the master boot record (MBR) with its own boot code. If you have any third-party boot managers installed, you will need to reactivate them after the Startup Recovery Manager has been activated. For Linux loaders (e.g. LiLo

Copyright © Acronis International GmbH, 2002-2016

and GRUB), you might consider installing them to a Linux root (or boot) partition boot record instead of MBR before activating Acronis Startup Recovery Manager.

UEFI boot mechanism is different from the BIOS one. Any OS loader or other boot program has its own boot variable that defines a path to the corresponding loader. All loaders are stored on a special partition called EFI System Partition. When you activate Acronis Startup Recovery Manager in UEFI-booted system, it changes the boot sequence by writing its own boot variable. This variable is added to the list of variables and does not change them. Since all loaders are independent and do not affect each other, there is no need to change anything before or after activating Acronis Startup Recovery Manager.

11.3 Try&Decide

When you turn Try&Decide on, your computer is in the Try mode. After that you can perform any potentially dangerous operations without worrying that you might damage your operating system, programs or data. When you turn Try&Decide off, you decide if you want to apply the changes to your computer or you want to discard them.

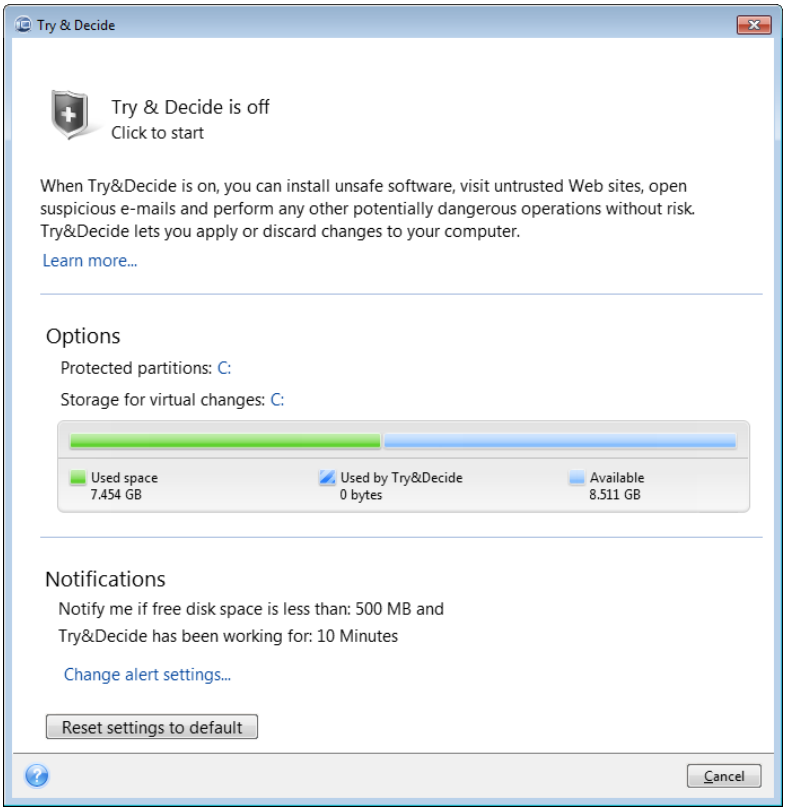
When Try&Decide can help

We recommend that you turn Try&Decide on before you try to:

- Change any system settings, when you are not sure how these changes may affect your computer.
- Install system updates, drivers, etc.
- Install unfamiliar applications.
- Open mail attachments from unknown senders.
- Visit websites that might contain potentially troublesome content.

Copyright © Acronis International GmbH, 2002-2016

Please remember that if you download e-mail from a POP mail server, create new files or edit existing documents while in the Try mode, and then decide to discard your changes, those files, document changes, and mail will no longer exist. In this case, save the new files and edited documents, for example, to a USB flash drive and unplug it before discarding the changes.


Try & Decide
Try & Decide is off
Click to start
When Try&Decide is on, you can install unsafe software, visit untrusted Web sites, open suspicious e-mails and perform any other potentially dangerous operations without risk. Try&Decide lets you apply or discard changes to your computer.
Learn more...
Options
Protected partitions: C:
Storage for virtual changes: C:
Used space
7.454 GB
Used by Try&Decide
0 bytes
Available
8.511 GB
Notifications
Notify me if free disk space is less than: 500 MB and
Try&Decide has been working for: 10 Minutes
Change alert settings...
Reset settings to default
Cancel

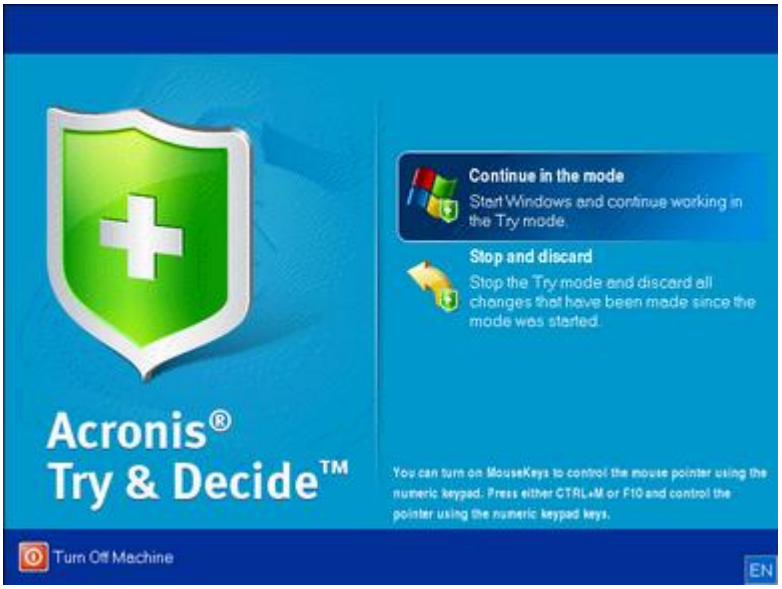
How Try&Decide works after a computer restart

You can leave the Try&Decide turned on as long as you like, because this mode "survives" across reboots of your operating system.

When your computer reboots for whatever reason while working in the Try mode, before booting of the operating system starts, you will be shown a dialog offering you two choices – stop the mode and discard changes or continue working in the mode. This will allow you to discard the changes that have resulted in a system crash. On the other hand, if you reboot, for example, after installing an application, you can continue working in the Try mode after starting Windows.

Copyright © Acronis International GmbH, 2002-2016

Every "soft" reboot of your computer while in the Try mode results in adding up to 500 MB of Try&Decide's housekeeping data into the storage selected for storing virtual changes.


Continue in the mode
Start Windows and continue working in the Try mode.
Stop and discard
Stop the Try mode and discard all changes that have been made since the mode was started.
Acronis®
Try & Decide™
You can turn on MouseKeys to control the mouse pointer using the numeric keypad. Press either CTRL+M or F10 and control the pointer using the numeric keypad keys.
Turn Off Machine
EN

Limitations in using Try&Decide

If you use Windows 7, Windows 8 or Windows 10, please, be aware that in the Try mode the program may use free disk space quite intensively, even when your computer is idle. This is due to housekeeping activities such as indexing that run in the background.

Please note that while working in the Try mode you will experience slowing down of the system performance. Furthermore, the process of applying changes may take a long time, especially if you leave the Try mode turned on days on end.

Please be aware that Try&Decide cannot track changes in disk partitions, so you will be unable to use the Try mode for virtual operations with partitions such as resizing partitions or changing their layout. In addition, you must not use the Try&Decide and disk defragmentation or disk error checking utilities at the same time, because this can irreparably corrupt the file system, as well as make the system disk unbootable.

When the Try mode is started, you won't be able to use the previously activated Acronis Startup Recovery Manager. Rebooting the computer in the Try mode will allow you to use Acronis Startup Recovery Manager again.

Try&Decide and Nonstop Backup cannot work simultaneously. Starting the Try mode suspends Nonstop Backup. Nonstop Backup will resume after you stop the Try mode.

When the Try mode is started, you won't be able to use the "Hibernate" power saving mode.

Try&Decide cannot be used for protecting dynamic disks.

Try&Decide cannot work when a partition in your system is encrypted with BitLocker.

Try&Decide cannot protect Acronis Secure Zone or use it as a storage for the virtual changes.

In this section

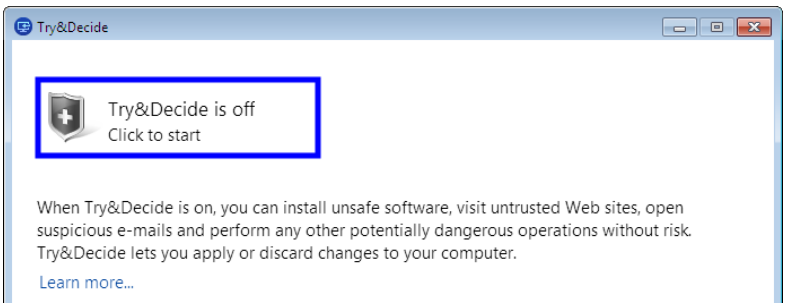
Using Try&Decide.....135
Try&Decide options and notifications 136
Try&Decide: typical use cases.....136

 Copyright © Acronis International GmbH, 2002-2016

11.3.1 Using Try&Decide

To use Try&Decide:

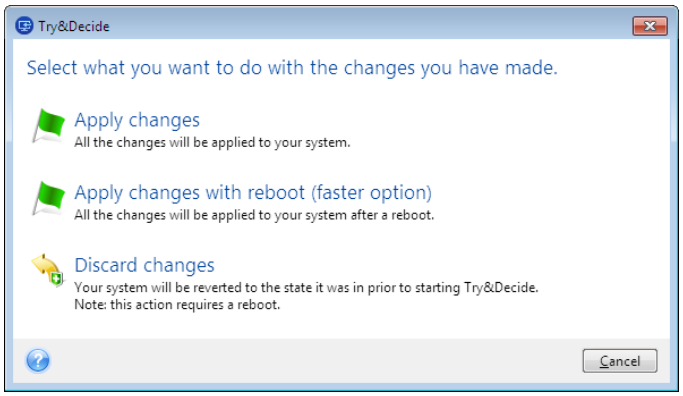
1. Start Acronis True Image.
2. In the **Tools** section, click **More tools**, and then double-click **Try&Decide**.
3. Set up the Try&Decide options, if necessary. Refer to Try&Decide options and notifications (p. 136) for details.
4. To start the Try mode, click the Try&Decide icon. The program starts tracking all changes made to the OS and files and temporarily stores all the changes on the selected disk.


Try&Decide
Try&Decide is off
Click to start
When Try&Decide is on, you can install unsafe software, visit untrusted Web sites, open suspicious e-mails and perform any other potentially dangerous operations without risk. Try&Decide lets you apply or discard changes to your computer.
Learn more...

5. Perform all the changes you wanted to try.

When the disk space in the location selected for storing virtual changes is minimal for applying the changes, the program asks you whether to apply or discard the changes. If you ignore the alert message, the program will automatically restart the system when the disk is full, and discard the changes.

6. To stop the Try mode, click the Try&Decide icon in the **Try&Decide** window.


Try&Decide
Select what you want to do with the changes you have made.
Apply changes
All the changes will be applied to your system.
Apply changes with reboot (faster option)
All the changes will be applied to your system after a reboot.
Discard changes
Your system will be reverted to the state it was in prior to starting Try&Decide.
Note: this action requires a reboot.
Cancel

7. Choose one of the following:
   - Select **Apply changes** if you want to keep the changes made to the system.
   - Select **Apply changes with reboot** if you want to speed up the applying process. When you click the button, Try&Decide restarts your computer and applies the changes during the reboot.
   - Select **Discard changes** if you want to return your system to the state it was in prior to turning on the Try mode.

*If you have chosen **Discard Changes** and rebooted the computer with multiple operating systems installed, you won't be able to boot other operating systems except the one used for working in the Try mode. A second reboot will recover the original MBR and make other operating systems bootable.*

Copyright © Acronis International GmbH, 2002-2016

11.3.2 Try&Decide options and notifications

You can change Try&Decide options in the Try&Decide window. To restore the default values of the settings, click Reset settings to default.

Protected partitions

To change this setting:

1. Click the partition letter next to the setting name. The Partition Selection window opens.
2. Select the partitions that you want to protect, and then click **OK**.

   By default, Try&Decide protects the system partition (Disk C), though you may choose to protect any other partitions in your system.

Storage for virtual changes

To change this setting:

1. Click the partition letter next to the setting name. The Storage for Virtual Changes window opens.
2. Select the partition that you want to use as a storage for virtual changes, and then click **OK**.

   By default, Try&Decide saves the information to a free space on Disk C.

When choosing to protect more than one partition, you cannot select one of the partitions to be protected to store virtual changes. In addition, you cannot select an external hard disk drive.

Notifications

To change the default notification settings, click **Change alert settings**. The Settings window opens.

- On free disk space remaining - If the amount of free space in the storage for virtual changes becomes less than the specified value, the program displays a notification message.
- On time elapsed since Try&Decide started - The program will notify you if Try&Decide has been working for longer than the period of time that you specified.

11.3.3 Try&Decide: typical use cases

The Try&Decide feature can help you in various circumstances, for example:

Software evaluation

Sometimes it may be useful to turn on the Try mode before installing new software. For example, we recommend that you turn it on when you want to:

- Choose antivirus software.

  There are known cases when installation of antivirus software cripples functionality of some applications or they may even refuse to launch after antivirus installation. You can test a trial version of the antivirus. If you encounter any problems, discard the changes in your system and try antivirus software from another vendor.
- Install a trial version of a program.

  It is well known that the "Add or Remove Programs" component of the Windows Control Panel cannot give a complete guarantee of cleanly uninstalling applications. If you do not like the program that you installed, discard the changes in your system. In this case, you can be sure that Try&Decide removed the program without a trace.

Copyright © Acronis International GmbH, 2002-2016

- Install suspicious software.

  If you do not trust the vendor of the software that you want to install, or when the source of the software is unknown, turn on the Try mode before installing this software. If anything goes wrong, discard the changes made in the Try mode.

File recovery

You have accidentally deleted some files and then emptied the Recycle Bin. Then you have remembered that the deleted files contained important data and now you are going to try to undelete them using the appropriate software. However, sometimes you may do something wrong while trying to recover deleted files, making things worse than before trying to recover them. So you can proceed as follows:

- Turn on the Try mode.
- Launch the file undelete utility.
- After the utility scans your disk in search of the deleted file or folder entries, it will present you the deleted entries it has found (if any) and offer you the opportunity to save whatever it can recover. There is always a chance that you might pick the wrong file and while recovering it the utility may overwrite the very file you are trying to recover. If not for the Try&Decide, this error would be fatal and the file would be lost irretrievably.
- But now you can just discard the changes made in the Try mode and make one more attempt to recover the files after turning on the Try mode again. Such attempts may be repeated until you are sure that you have done your best in trying to recover the files.

Web privacy

Suppose you do not want anybody to know, which Web sites you have visited or which pages you have opened - we all have the right to privacy. But the problem is that to make your Web surfing more comfortable and fast, the system stores this information and much more: cookies you have received, search engine queries you have made, URLs you have typed, etc. in special hidden files. And such information is not deleted completely when you clear your temporary Internet files, delete cookies, clear history of the recently opened Web pages using the browser's tools. So snoopers may be able to view the information using special software.

Turn on the Try mode and surf the Web as you please. Afterwards, if you want to remove all traces of your activity, discard the changes made in the Try mode.

11.4 Acronis Secure Zone

The Acronis Secure Zone is a special secure partition that you can create on your computer for storing backups. The Acronis Secure Zone has a FAT32 file system.

Acronis Secure Zone in File Explorer

When you create an Acronis Secure Zone, it is displayed in the **Other** section of File Explorer. You can navigate through the Acronis Secure Zone as an ordinary partition.

Right-click a specific backup or a backup version to view all available operations:

- Explore
- Mount (for image backups)
- Recover
- Validate
- Update

Copyright © Acronis International GmbH, 2002-2016

- Remove
- View the version's details

If Acronis Secure Zone is password-protected, any operation, except viewing version details, requires entering the password.

Acronis Secure Zone cleanup

If there is not enough space in the Acronis Secure Zone for a new backup, you can:

- Cancel the backup operation, increase the size of the Acronis Secure Zone, and then run the backup again.
- Cancel the backup operation, manually delete some backups in the Acronis Secure Zone, and then run the backup again.
- Confirm that you want to automatically delete the oldest backup of the same type (file-level or disk-level) with all subsequent incremental and differential versions. After that, if free space is still insufficient, Acronis True Image asks for confirmation and will delete the next full backup. This will repeat until there is enough free space for the new backup. If after deleting all the previous backups there is still not enough space, the backup will be canceled.

To prevent the zone overflow, we recommended that you select the **When not enough space in ASZ, delete the oldest backup** check box in the scheduled backup options. Refer to Error handling (p. 59) for details.

You can use the Acronis Secure Zone as the storage for virtual system changes in the Try mode. The Try&Decide data will be automatically cleaned up after you stop a Try&Decide session.

Acronis True Image does not delete nonstop backup versions in the Acronis Secure Zone automatically. Such versions can only be deleted manually. For more information see Acronis Nonstop Backup data storage (p. 36).

In this section

Creating and managing Acronis Secure Zone 138
Acronis Secure Zone location.....139
Size of Acronis Secure Zone 140
Acronis Secure Zone protection.....140
Removing Acronis Secure Zone.....141

11.4.1 Creating and managing Acronis Secure Zone

To create or modify the Acronis Secure Zone:

1. Click the **Start** button —> **Acronis** (product folder) —> **True Image** —> **Tools and Utilities** —> **Acronis Secure Zone**.

   The Manage Acronis Secure Zone wizard opens.
2. Perform one of the following:

- If you want to create the Acronis Secure Zone, specify its location (p. 139) and size (p. 140).
- If you want to modify the Acronis Secure Zone, select an action:
  - Increase or decrease size (p. 139)
  - Remove (p. 141)
  - Change password (p. 140)

    Then follow the wizard steps.

 Copyright © Acronis International GmbH, 2002-2016

1. On the **Finish** step, click **Proceed**.

Note: This operation may require a computer restart.

11.4.2 Acronis Secure Zone location

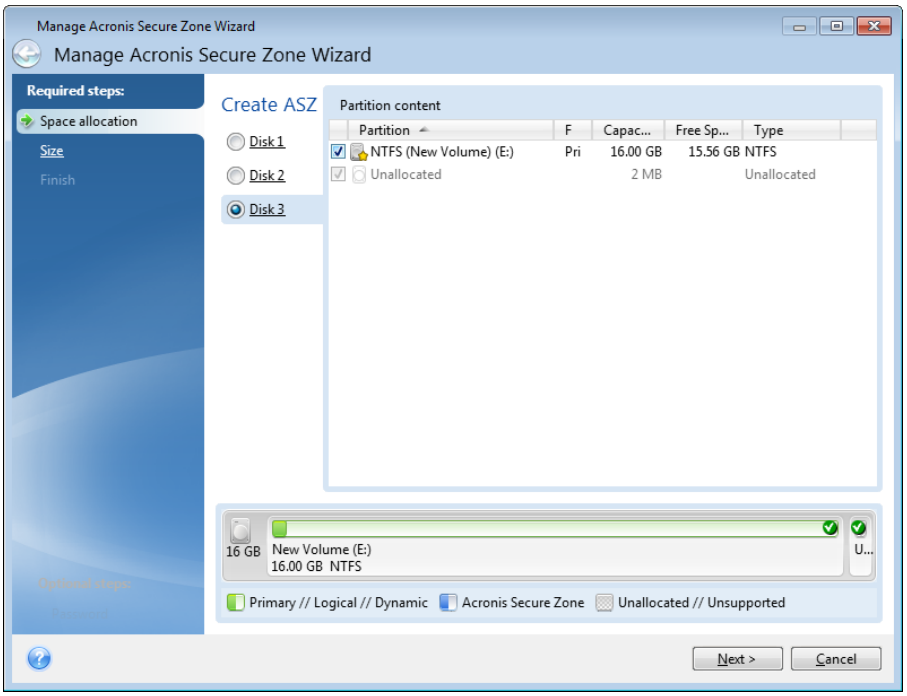
Creating the Acronis Secure Zone

To specify a location for the Acronis Secure Zone:

1. Select a hard disk drive to create the Acronis Secure Zone on.
2. Select one or more partitions from which unallocated and/or free space will be taken. The chosen partitions will be resized if necessary to give space to the Acronis Secure Zone.

   The Acronis Secure Zone cannot be created on dynamic disks and volumes.

3. Click **Next**.



Increasing or decreasing the size of the Acronis Secure Zone

To increase/decrease the size of the Acronis Secure Zone:

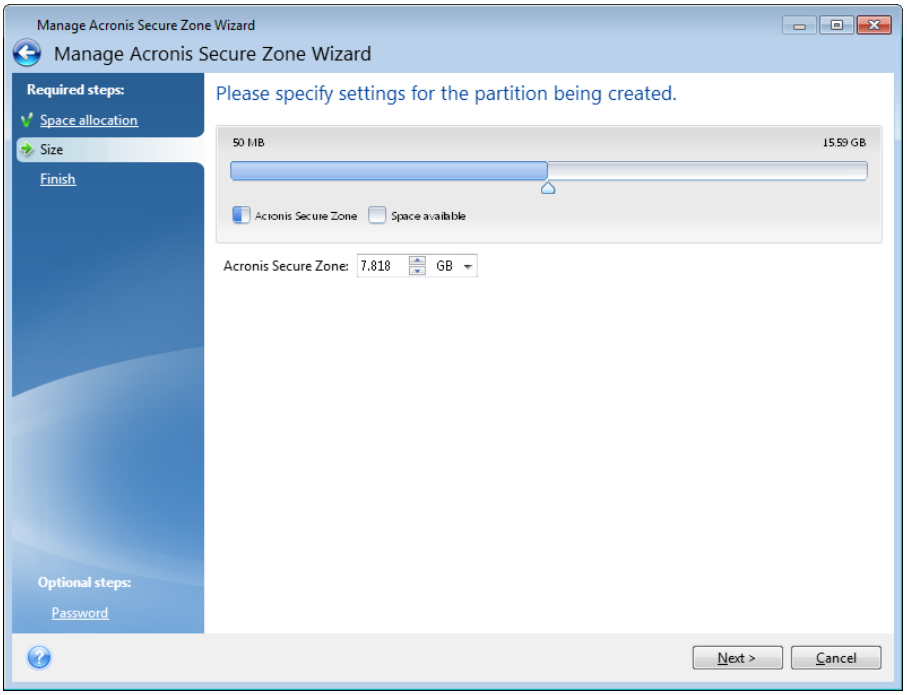
1. Select the partitions from which space will be used to increase the size of the Acronis Secure Zone, or that will receive free space after the size of the Acronis Secure Zone is reduced. You can also select partitions with unallocated space.
2. Click **Next**.

Copyright © Acronis International GmbH, 2002-2016

11.4.3 Size of Acronis Secure Zone

To specify the size of the Acronis Secure Zone:

Drag the slider to the appropriate position or type an exact value.



The minimum size is about 50 MB, depending on the geometry of the hard disk. The maximum size is equal to the disk's unallocated space plus the total free space on all partitions selected at the previous step.

When creating/enlarging the Acronis Secure Zone, the program will first use the unallocated space. If the unallocated space is not enough to achieve the desired size, the selected partitions will be decreased in size. Resizing of partitions may require the computer to be rebooted.

When reducing the size of the Acronis Secure Zone, if there is any unallocated space on the hard disk, it will be allocated to the selected partitions along with the space freed up from the Acronis Secure Zone. Thus, no unallocated space will remain on the disk.

Warning! *Reducing a system partition to the minimum size may prevent your operating system from booting-up.*

11.4.4 Acronis Secure Zone protection

You can set up password protection for the Acronis Secure Zone in order to prevent it from unauthorized access.

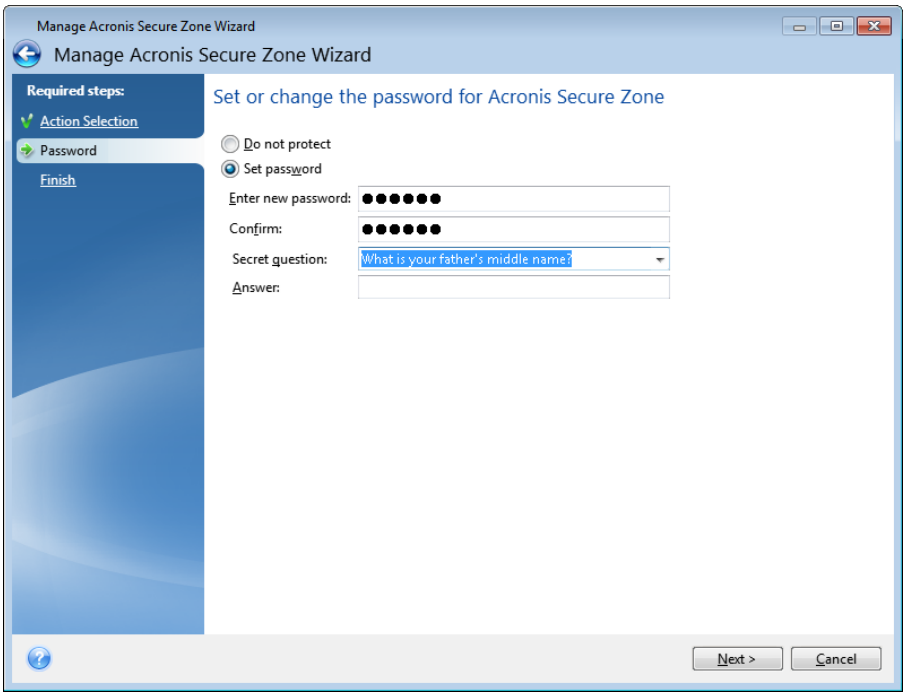
The program will ask for the password at any operation relating to the Acronis Secure Zone such as data backup and recovery, mounting images or validating backups in the Acronis Secure Zone, resizing and deleting the Acronis Secure Zone.

To set a password for the Acronis Secure Zone:

1. Select **Set password**.
2. Type the password in the **Password** field.

Copyright © Acronis International GmbH, 2002-2016

3. Retype the previously entered password in the **Confirm** field.
4. [Optional step] You can also select a secret question that will be asked in case you forget the password. Select a secret question from the list and enter an answer to it.
5. Click **Next** to continue.



Acronis True Image repair or update will not affect the password. However, if the program is removed and then installed again while keeping the Acronis Secure Zone on the disk, the password to the Acronis Secure Zone will be reset.

11.4.5 Removing Acronis Secure Zone

Acronis Secure Zone deletion will automatically destroy all backups stored in the zone.

Select the partitions to which you want to add the space freed up from Acronis Secure Zone. If you select several partitions, the space will be distributed proportionally to each partition's size.

Also, you can choose to remove the Acronis Secure Zone while uninstalling the program.

11.5 Adding a new hard disk

If you do not have enough space for your data, you can either replace the old disk with a new higher-capacity one, or add a new disk only to store data, leaving the system on the old disk.

To add a new hard disk:

1. Shut down your computer, and then install the new disk.
2. Turn on your computer.
3. Click the **Start** button —> **Acronis** (product folder) —> **True Image** —> **Tools and Utilities** —> **Add New Disk**.
4. Follow the wizard steps.

Copyright © Acronis International GmbH, 2002-2016

5. On the **Finish** step, ensure that the configured disk layout suits your needs, and then click **Proceed**.

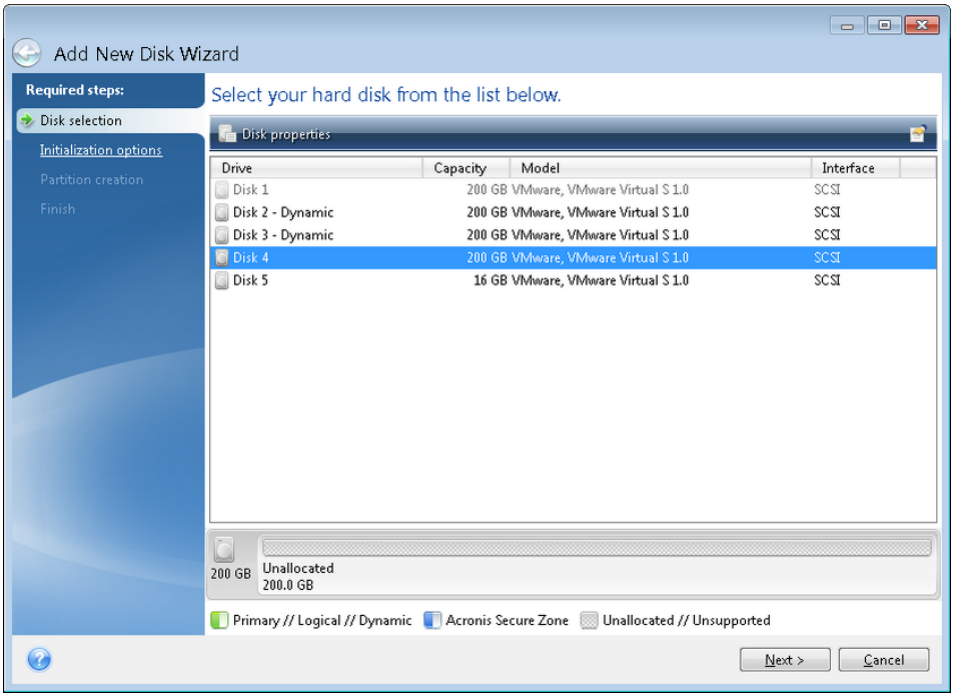
In this section

Selecting a hard disk 142
Selecting initialization method 143
Creating new partitions.....143

11.5.1 Selecting a hard disk

Select the disk that you have added to the computer. If you have added several disks, select one of them and click **Next** to continue. You can add the other disks later by restarting the Add New Disk Wizard.

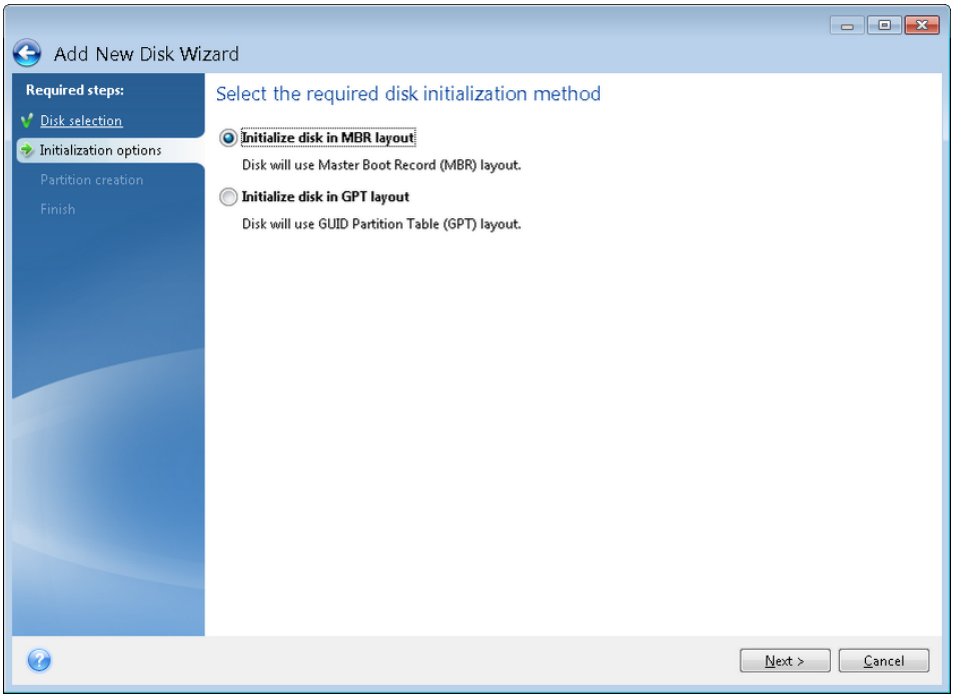
If there are any partitions on the new disk, Acronis True Image will warn you that these partitions will be deleted.


Add New Disk Wizard
Required steps:
Disk selection
Initialization options
Partition creation
Finish
Select your hard disk from the list below.
Disk properties
Drive
Capacity
Model
Interface
Disk 1 200 GB VMware, VMware Virtual S 1.0 SCSI
Disk 2 - Dynamic 200 GB VMware, VMware Virtual S 1.0 SCSI
Disk 3 - Dynamic 200 GB VMware, VMware Virtual S 1.0 SCSI
Disk 4 200 GB VMware, VMware Virtual S 1.0 SCSI
Disk 5 16 GB VMware, VMware Virtual S 1.0 SCSI
200 GB
Unallocated
200.0 GB
Primary // Logical // Dynamic
Acronis Secure Zone
Unallocated // Unsupported
Next >
Cancel

Copyright © Acronis International GmbH, 2002-2016

11.5.2 Selecting initialization method

Acronis True Image supports both MBR and GPT partitioning. GUID Partition Table (GPT) is a new hard disk partitioning method providing advantages over the old MBR partitioning method. If your operating system supports GPT disks, you can select the new disk to be initialized as a GPT disk.



- To add a GPT disk, click **Initialize disk in GPT layout**.
- To add an MBR disk, click **Initialize disk in MBR layout**.

*If you use a 32-bit version of Windows XP, the GPT initialization method will be unavailable and the **Initialization options** step will be absent.*

After selecting the required initialization method click **Next**.

11.5.3 Creating new partitions

To use the space on a hard disk, it must be partitioned. Partitioning is the process of dividing the hard disk's space into logical divisions which are called partitions. Each partition may function as a separate disk with an assigned drive letter, its own file system, etc.

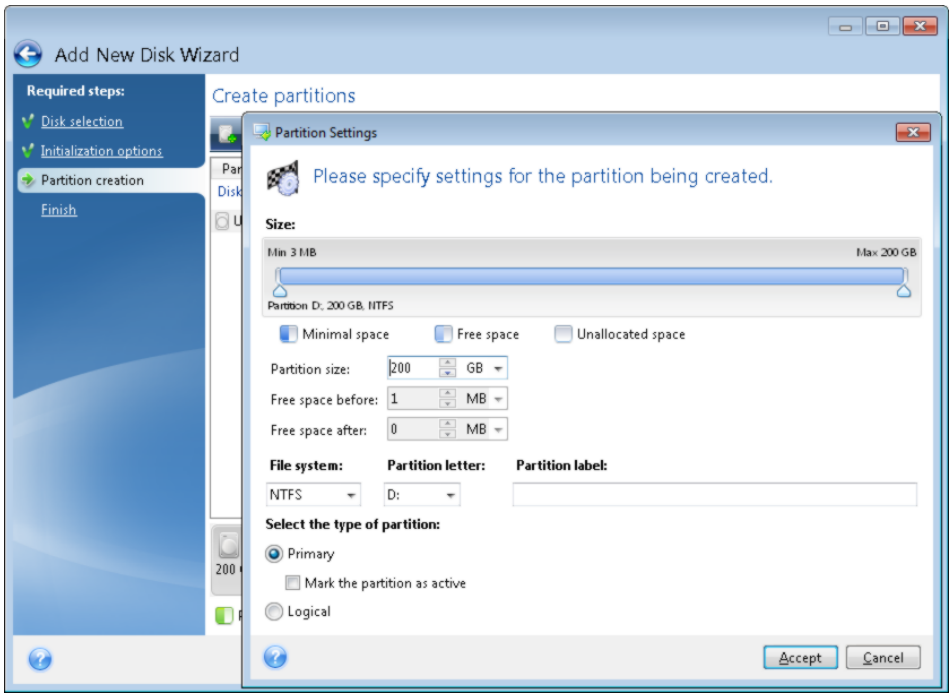
To create a new partition:

1. On the **Partition creation** step of the wizard, select the unallocated space, and then click **Create new partition**.
2. Specify the following settings for the partition being created:
   - Size and position
   - File system
   - Partition type (available only for MBR disks)
   - Partition letter and label

   Refer to Partition settings (p. 144) for details.

Copyright © Acronis International GmbH, 2002-2016

3. Click **Accept**.



11.5.3.1 Partition settings

Size

To resize the partition, perform one of the following:

- Point to the partition border. When the pointer becomes a double-headed arrow, drag the pointer to enlarge or reduce the partition size.
- Type the desired partition size in the **Partition Size** field.

To relocate the partition, perform one of the following:

- Drag the partition to a new position.
- Type the desired size in either the **Free space before** or **Free space after** field.

When you create partitions, the program may reserve some unallocated space for system needs in front of the created partitions.

File System

You can either leave the partition unformatted, or choose between the following file system types:

- **NTFS** is a native file system for Windows NT, Windows 2000, Windows XP, and later operating systems. Choose it if you use these operating systems. Note, that Windows 95/98/Me and DOS cannot access NTFS partitions.
- **FAT 32** is an improved 32-bit version of the FAT file system that supports volumes up to 2 TB.
- **FAT 16** is a DOS native file system. Most operating systems recognize it. However, if your disk drive is more than 4 GB, it is not possible to format it in FAT16.
- **Ext2** is a Linux native file system. It is fast enough, but it is not a journaling file system.

Copyright © Acronis International GmbH, 2002-2016

- **Ext3 –** officially introduced with Red hat Linux version 7.2, Ext3 is a Linux journaling file system. It is forwards and backwards compatible with Linux Ext2. It has multiple journaling modes, as well as broad, cross platform compatibility in both 32-bit and 64-bit architectures.
- **Ext4** is a new Linux file system. It has improvements in comparison to ext3. It is fully backward compatible with ext2 and ext 3. However, ext3 has only partial forward compatibility with ext4.
- **ReiserFS** is a journaling file system for Linux. Generally it is more reliable and faster than Ext2. Choose it for your Linux data partition.
- **Linux Swap** is a swap partition for Linux. Choose it if you want to add more swap space using Linux.

Partition letter

Select a letter to be assigned to the partition. If you select **Auto**, the program assigns the first unused drive letter in alphabetical order.

Partition label

Partition label is a name, assigned to a partition so that you can easily recognize it. For example, a partition with an operating system could be called System, a data partition — Data, etc. Partition label is an optional attribute.

Partition type (these settings are available only for MBR disks)

You can define the new partition as primary or logical.

- **Primary** - choose this parameter if you are planning to boot from this partition. Otherwise, it is better to create a new partition as a logical drive. You can have only four primary partitions per drive, or three primary partitions and one extended partition.

  Note: If you have several primary partitions, only one will be active at a time, the other primary partitions will be hidden and won't be seen by the OS.

  - **Mark the partition as active** - select this check box if you are planning to install an operating system on this partition.
- **Logical** - choose this parameter if you don't intend to install and start an operating system from the partition. A logical drive is part of a physical disk drive that has been partitioned and allocated as an independent unit, but functions as a separate drive.

11.6 Security and Privacy Tools

In this section

Acronis DriveCleanser 145
System Clean-up 149
Hard Disk Wiping methods 155

11.6.1 Acronis DriveCleanser

Acronis DriveCleanser allows you to permanently destroy all data on selected hard disks and partitions. For the destruction, you can use one of the preset algorithms or create your own. Refer to Algorithm selection (p. 147) for details.

 Copyright © Acronis International GmbH, 2002-2016

Why do I need it?

When you format your old hard drive before throwing it away, the information is not destroyed permanently and it can still be retrieved. This is a way that your personal information can end up in the wrong hands. To prevent this, we recommend that you use Acronis DriveCleanser when you:

- Replace your old hard drive with a new one and do not plan to use the old drive any more.
- Give your old hard drive to your relative or friend.
- Sell your old hard drive.

How to use Acronis DriveCleanser

To permanently destroy data on your disk:

1. Click the **Start** button —> **Acronis** (product folder) —> **True Image** —> **Tools and Utilities** —> **DriveCleanser**.

   The Acronis DriveCleanser wizard opens.
2. On the **Source selection** step, select the disks and partitions that you want to wipe. Refer to Source selection (p. 146) for details.
3. On the **Algorithm selection** step, select an algorithm that you want to use for the data destruction. Refer to Algorithm selection (p. 147) for details.
4. [optional step] You can create your own algorithm. Refer to Creating custom algorithm for details.
5. [optional step] On the **Post-wiping actions** step, choose what to do with the partitions and disk when the data destruction is complete. Refer to Post-wiping actions (p. 149) for details.
6. On the **Finish** step, ensure that the configured settings are correct. To start the process, select the **Wipe the selected partitions irreversibly** check box, and then click **Proceed**.

Be aware that, depending on the total size of selected partitions and the selected data destruction algorithm, the data destruction may take many hours.

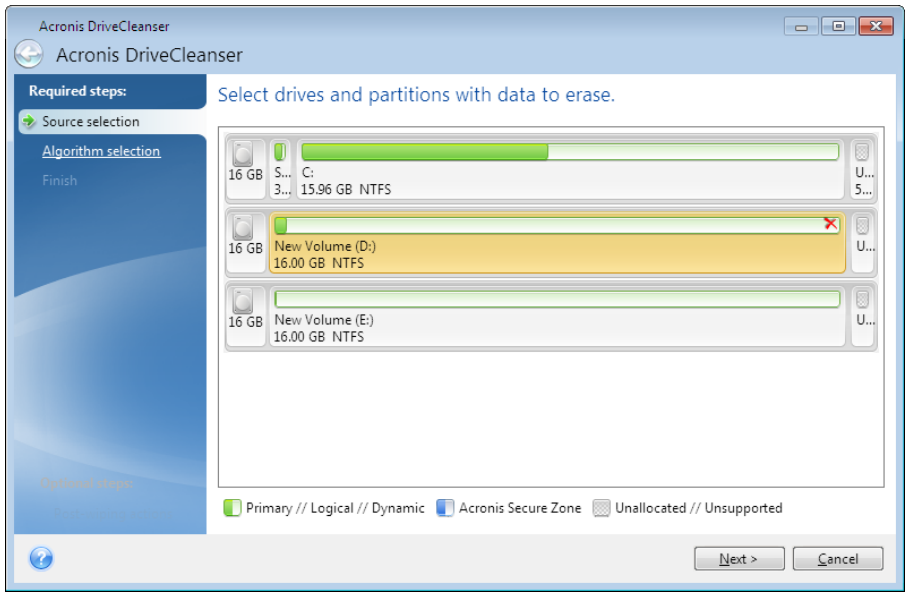
11.6.1.1 Source selection

On the **Source selection** step, select partitions and disks where you want to destroy data:

- To select partitions, click the corresponding rectangles. The red mark ( ) indicates that the partition is selected.

Copyright © Acronis International GmbH, 2002-2016

- To select an entire hard disk, click the disk icon ( ).

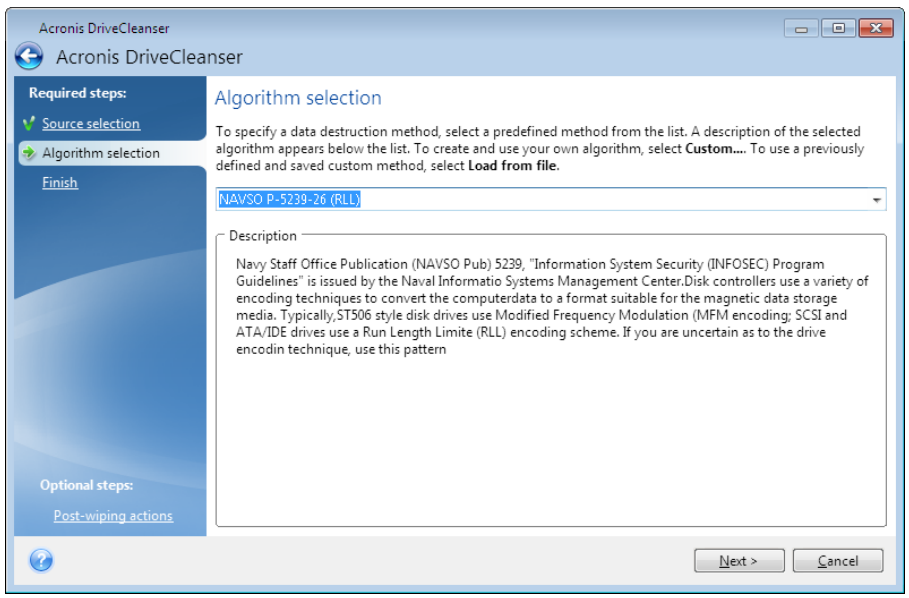


Acronis DriveCleanser cannot wipe partitions on dynamic and GPT disks, so they will not be shown.

11.6.1.2 Algorithm selection

On the **Algorithm selection** step, perform one of the following:

- To use one of the preset algorithms, select the desired algorithm. Refer to Hard Disk Wiping Methods (p. 155) for details.
- [For advanced users only] To create a custom algorithm, select **Custom**. Then continue creating on the **Algorithm definition** step. Afterwards, you will be able to save the created algorithm to a file with *.alg extension.
- To use a previously saved custom algorithm, select **Load from file** and select the file containing your algorithm.


Acronis DriveCleanser
Acronis DriveCleanser
Required steps:
Source selection
Algorithm selection
Finish
Optional steps:
Post-wiping actions
Algorithm selection
To specify a data destruction method, select a predefined method from the list. A description of the selected algorithm appears below the list. To create and use your own algorithm, select Custom.... To use a previously defined and saved custom method, select Load from file.
NAVSO P-5239-26 (RLL)
Description
Navy Staff Office Publication (NAVSO Pub) 5239, "Information System Security (INFOSEC) Program Guidelines" is issued by the Naval Informatio Systems Management Center.Disk controllers use a variety of encoding techniques to convert the computerdata to a format suitable for the magnetic data storage media. Typically,ST506 style disk drives use Modified Frequency Modulation (MFM encoding; SCSI and ATA/IDE drives use a Run Length Limite (RLL) encoding scheme. If you are uncertain as to the drive encodin technique, use this pattern
Next >
Cancel

Copyright © Acronis International GmbH, 2002-2016

Creating custom algorithm

Algorithm definition

The **Algorithm definition** step shows you a template of the future algorithm.

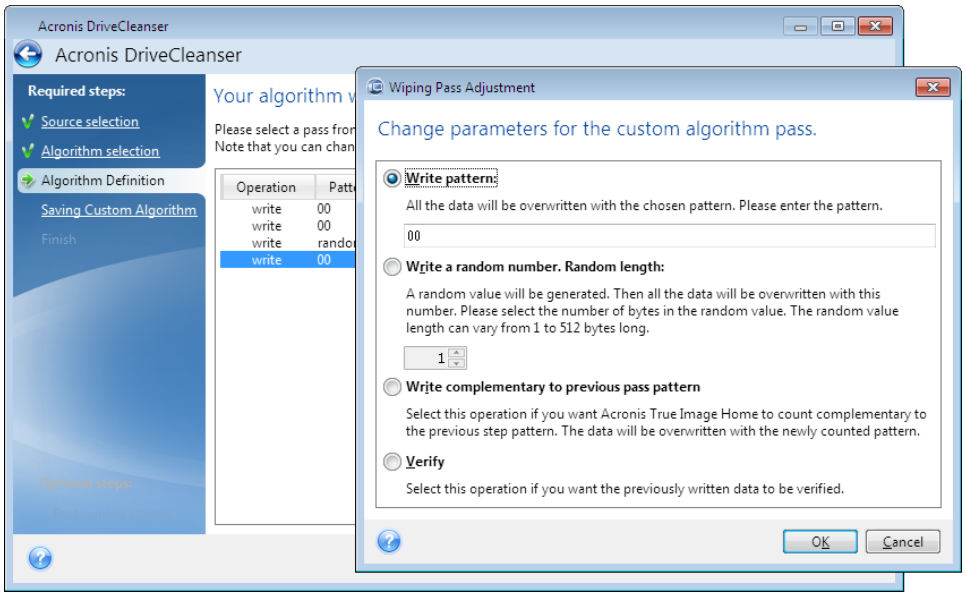
The table has the following legend:

- The first column contains the type of operation (to write a symbol to disk; and to verify written).
- The second column contains the pattern of data to be written to disk.

Each line defines an operation that will be performed during a pass. To create your algorithm, add as many lines to the table that you think will be enough for secure data destruction.

To add a new pass:

1. Click **Add**. The Wiping Pass Adjustment window opens.


Acronis DriveCleanser
Acronis DriveCleanser
Required steps:
Source selection
Algorithm selection
Algorithm Definition
Saving Custom Algorithm
Finish
Operation
write 00
write 00
write
write 00
Wiping Pass Adjustment
Change parameters for the custom algorithm pass.
Write pattern:
All the data will be overwritten with the chosen pattern. Please enter the pattern.
00
Write a random number. Random length:
A random value will be generated. Then all the data will be overwritten with this number. Please select the number of bytes in the random value. The random value length can vary from 1 to 512 bytes long.
1
Write complementary to previous pass pattern
Select this operation if you want Acronis True Image Home to count complementary to the previous step pattern. The data will be overwritten with the newly counted pattern.
Verify
Select this operation if you want the previously written data to be verified.
OK
Cancel

2. Choose an option:
   - **Write pattern**

     Enter a hexadecimal value, for example, a value of this kind: 0x00, 0xAA, or 0xCD, etc. These values are 1 byte long, but they may be up to 512 bytes long. Except for such values, you may enter a random hexadecimal value of any length (up to 512 bytes).

     If the binary value is represented by the 10001010 (0x8A) sequence, then the complementary binary value will be represented by the 01110101 (0x75) sequence.

   - **Write a random number**

     Specify the length of the random value in bytes.

   - **Write complementary to previous pass pattern**

     Acronis True Image adds a complementary value to the one written to disk during the previous pass.

   - **Verify**

     Acronis True Image verifies the values written to disk during the previous pass.
3. Click **OK**.

Copyright © Acronis International GmbH, 2002-2016

To edit an existing pass:

1. Select the corresponding line, and then click **Edit**.
   The Wiping Pass Adjustment window opens.

   Note: When you select several lines, the new settings will be applied to all of the selected passes.

2. Change the settings, and then click **OK**.

Saving algorithm to a file

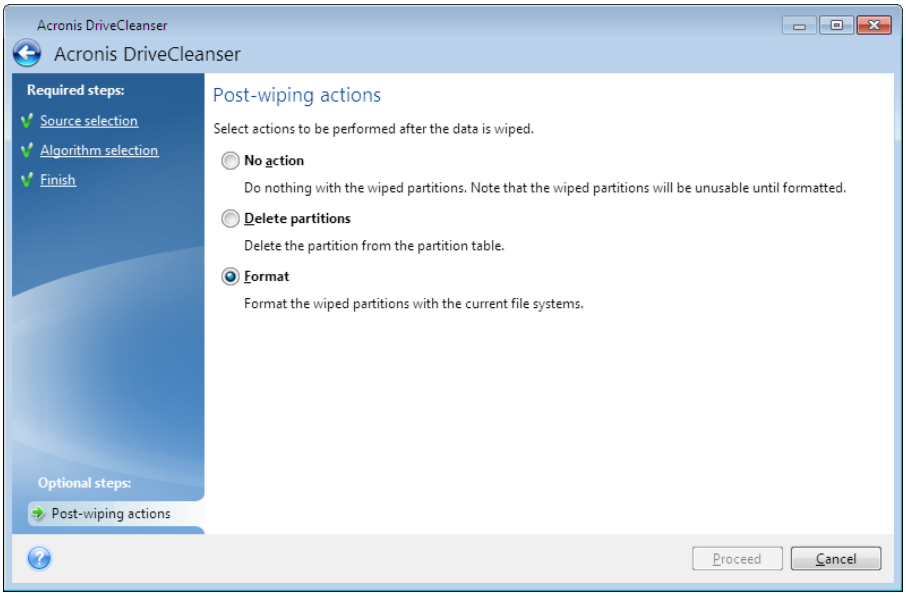
To save the created algorithm to a file in order to use this algorithm afterwards:

1. On the **Saving custom algorithm** step, select **Save to a file**, and then click **Next**.
2. In the window that opens, specify the file name and location, and then click **OK**.

11.6.1.3 Post-wiping actions

In the Post-wiping actions window, you can select actions to be performed on the partitions selected for data destruction. Acronis DriveCleanser offers you three options:

- **No action** — just destroy data using the algorithm selected below
- **Delete partition** — destroy data and delete partition
- **Format** — destroy data and format partition (default).



11.6.2 System Clean-up

The System Clean-up wizard enables you to securely remove all traces of your PC actions, including user names, passwords, and other personal information.

It can carry out the following operations:

- Securely destroy data in the **Windows Recycle Bin**
- Remove **temporary files** from appropriate Windows folders
- Clean up **hard disk free space** of any traces of information previously stored on it
- Remove traces of **file and computer searches** on connected disks and computers in the local area network

Copyright © Acronis International GmbH, 2002-2016

- Clean the **recently used documents** list
- Clean the **Windows Run** list
- Clean the **opened/saved files** history
- Clean the list of network places to which the user has connected using **network credentials**
- Clean the **Windows prefetch directory**, where Windows stores information about programs you have executed and run recently

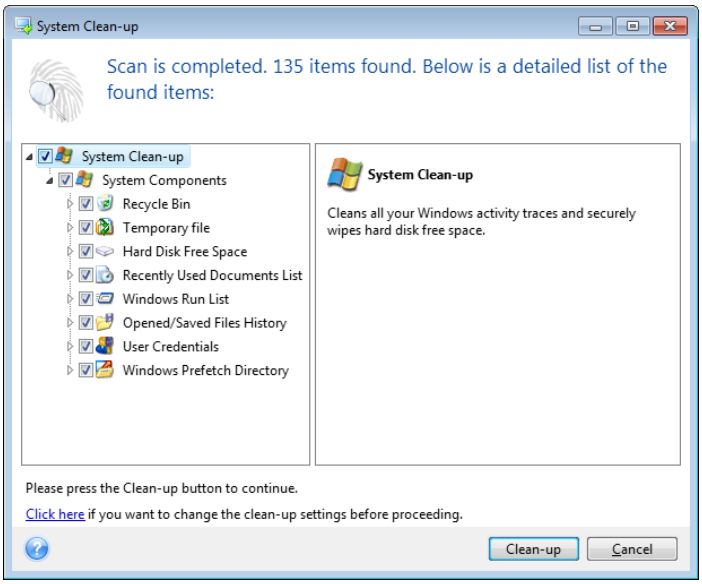
Windows 7 and later operating systems do not store information on file and computer searches. Furthermore, information on opened/saved files is stored differently in the registry, so the wizard shows this information in a different way.

*****

Please, be aware that Windows stores passwords until the session ends, so cleaning the list of network user credentials will not take effect until you end the current Windows session by logging out or by rebooting the computer.

To start the System Clean-up wizard, click the **Start** button —> **Acronis** (product folder) —> **True Image** —> **Tools and Utilities** —> **System Clean-up**.

After you start the wizard, it will search for any traces of user actions stored by Windows. When the search is finished, its results will be available at the top of the wizard window.


System Clean-up
Scan is completed. 135 items found. Below is a detailed list of the found items:
System Clean-up
System Components
Recycle Bin
Temporary file
Hard Disk Free Space
Recently Used Documents List
Windows Run List
Opened/Saved Files History
User Credentials
Windows Prefetch Directory
System Clean-up
Cleans all your Windows activity traces and securely wipes hard disk free space.
Please press the Clean-up button to continue.
Click here if you want to change the clean-up settings before proceeding.
Clean-up
Cancel

You can view the search results and manually select the items you wish to remove.

If you want to change the default system clean-up settings, click the corresponding link in the first window of the System Clean-up wizard.

Click **Clean-up** to launch removing the found items.

11.6.2.1 Clean-up settings

In the clean-up settings window you can change the clean-up settings for every system component. Some of these settings apply to all components.

Copyright © Acronis International GmbH, 2002-2016

To change the clean-up settings for a component:

- Expand the **System Components** item in the tree and select the component clean-up settings which you need to change. You can enable or disable scanning of the component by the Clean-up wizard. To do this, select or clear the **Enable** check box.

  If required, you can also expand a component and customize the desired data destruction method, files to clean, clean-up registry search strings you have used for finding computers in the local network, etc. To do this, click the triangle near the component, select an option from the list and specify the settings.
- After you set the desired components' properties, click **OK** to save your settings. These settings will be used as default next time you launch the Clean-up wizard.

If you have already changed the clean-up settings before, you can always return to the program defaults by clicking the **Restore Defaults** button.

System components:

- Recycle Bin
- Temporary files
- Hard disk free space
- Find Computer list
- Find File list
- Recently Used Documents list
- Windows Run List
- Opened/saved files history
- User Credentials
- Windows Prefetch Directory

11.6.2.2 Default clean-up options

The default clean-up options are available by clicking the **Click to change this setting…** link on the **Data Destruction Method** option page.

To change the default clean-up options:

- Choose on the tree the component clean-up settings which you need to change.
- After you change the options, click **OK** to save your settings.

If you have already changed the clean-up settings before, you can always return to the program defaults by clicking the **Restore Defaults** button.

General

By default, the summary dialog window is displayed after each clean-up procedure ends (the **Show summary** check box is selected). If you do not need this window to be displayed, uncheck the box.

Clean-up options

System Clean-up utilizes a number of the most popular data destruction methods. Here, you can select the common data destruction method which will be used by default for all other components.

The data destruction methods are described in detail in Hard Disk Wiping Methods (p. 155) of this guide.

Copyright © Acronis International GmbH, 2002-2016

11.6.2.3 Specific clean-up options

You can customize the following clean-up options:

- Data destruction method
- Default options
- Files
- Drive free space
- Computers
- Commands
- Network places filter

Data destruction method

System Clean-up utilizes a number of the most popular data destruction methods. Here, you need to select the desired data destruction method.

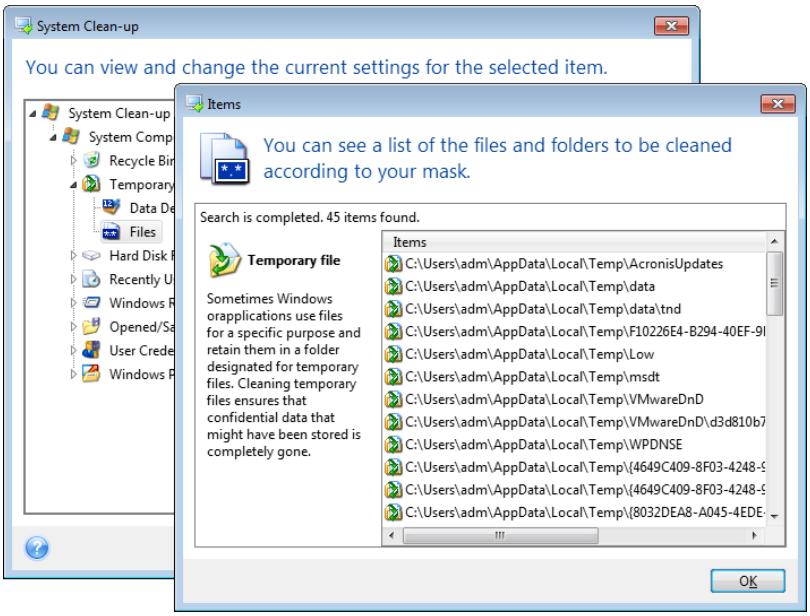
- **Use common method** - if you leave this parameter selected, the program will use the default method (the initial setting is Fast method).

  If you need another destruction method to be set as a default, click on the corresponding link.
- **Use custom method for this component** - selecting this parameter allows you to choose one of the preset data destruction methods from the drop-down list.

The data destruction methods are described in detail in Hard Disk Wiping Methods (p. 155) of this guide.

Files

The Files setting defines the names of files to clean with System Clean-up wizard and can be used with a search string.


System Clean-up
You can view and change the current settings for the selected item.
Items
You can see a list of the files and folders to be cleaned according to your mask.
Search is completed. 45 items found.
Temporary file
Sometimes Windows orapplications use files for a specific purpose and retain them in a folder designated for temporary files. Cleaning temporary files ensures that confidential data that might have been stored is completely gone.
Items
C:\Users\adm\AppData\Local\Temp\AcronisUpdates
C:\Users\adm\AppData\Local\Temp\data
C:\Users\adm\AppData\Local\Temp\data\tnd
C:\Users\adm\AppData\Local\Temp\Low
C:\Users\adm\AppData\Local\Temp\msdt
C:\Users\adm\AppData\Local\Temp\VMwareDnD
C:\Users\adm\AppData\Local\Temp\WPDNSE
OK

Copyright © Acronis International GmbH, 2002-2016

Under the Windows operating system, a search string can represent a full or partial filename. A search string can contain any alphanumeric symbols, including commas and Windows wildcard symbols, and can have values similar to the following:

- *.* – to clean all files with any file names and extensions.
- *.doc – to clean all files with a specific extension – Microsoft document files in this case .
- read*.* – to clean all files with any extensions, and names beginning with "read".
- read?.* – to clean all files having five-letter names and any extensions, names beginning with "read"; the fifth letter is random.

  The last search string, for example, will result in the removal of read1.txt, ready.doc files, but readyness.txt will remain with its longer name (excluding the extension)

You can enter several different search strings separated by semicolons; for example:

.bak;.tmp;*.~~~ (without spaces between the search strings)

All files with names corresponding to at least one of the search strings will be cleaned.

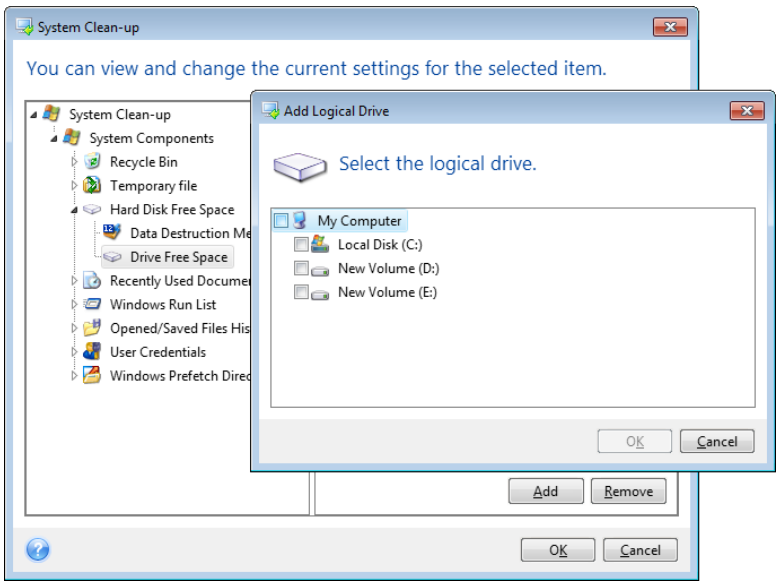
Upon entering the Files setting value, you can browse the files matching the search strings. To do this, click **Show Files**. You will see a window with the names of the found files. These files will be cleaned.

Drive free space

Here you can manually specify physical and/or logical drives to clean up free space on. By default, System Clean-up cleans up free space on all available drives.

If you want to change the settings of this parameter, you can use the **Remove** button to delete from the list the drives you don't need to clean free space on.

If you wish to add these drives to the list again, use the **Add** button.



Computers

The **Computers** setting is used for cleaning up the registry search strings you have used for finding computers in the local network. These strings keep information on what has interested you in the network. These items should also be deleted to maintain confidentiality.

Copyright © Acronis International GmbH, 2002-2016

The **Computers** setting is similar to the **Files** setting. It is a string that can contain any number of full or partial computer names separated by semicolons. The deletion of computer search strings is based on a comparison with the **Computers** setting value according to Windows rules.

If you simply need to delete all local network computer search strings (suitable in most cases), just leave the default value of this setting. To restore the default settings:

- Select the **Find Computer List** component
- Make sure the **Enable** check box is selected
- Select the **Computers** setting; make sure its text box is clear.

As a result, all computer search strings will be deleted from the registry.

After entering the **Computers** setting value, you can browse the search strings found by the System Clean-up Wizard in the registry. To do so, click **Show Computers**. You will see the window with full and partial computer names searched for in the network. These items will be deleted.

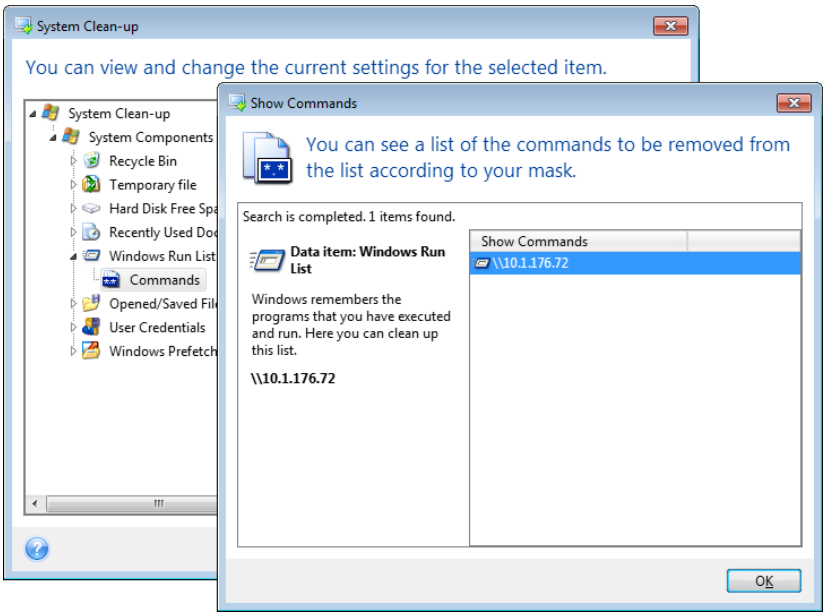
"Commands" setting

Here you can select the commands to remove during **Windows Run List** clean-up.

This template can contain any command names or their parts separated by semicolons, e.g.:

help; cmd; reg

This will result in removing commands with names corresponding to or containing any of the names or parts of names you entered.


System Clean-up
You can view and change the current settings for the selected item.
System Clean-up
System Components
Recycle Bin
Temporary file
Hard Disk Free Spa
Recently Used Doc
Windows Run List
Commands
Opened/Saved File
User Credentials
Windows Prefetch
Show Commands
You can see a list of the commands to be removed from the list according to your mask.
Search is completed. 1 items found.
Data item: Windows Run List
Windows remembers the programs that you have executed and run. Here you can clean up this list.
\\10.1.176.72
Show Commands
\\10.1.176.72
OK

Network places filter

Here you can enter (separated by semicolons) any hostnames or IP addresses of network places, servers, FTP servers, network shares, etc. to which you have made connection by supplying network credentials (a user name and password). While entering hostnames and IP addresses you can use * and ? wildcards.

Copyright © Acronis International GmbH, 2002-2016

Click **Show network places** to view the list of network places that you visited using the credentials you want to delete.

11.6.2.4 Preview

When the scanning is finished, its results will be available in the upper part of the wizard window. By default, all system components are scanned for clean-up. If you want to customize which of the system components should be scanned and which should not, change the default clean-up settings.

You can view the search results and manually select/unselect the items you wish to clean up/keep. In order to help you with making the right choice, all the components are provided with brief descriptions. Just click on the component's name and its description will be displayed in the right side of the window.

To select/unselect a component

- Expand the **System Components** item in the System Clean-up tree and make sure that the component you wish to clean up is selected. If you do not want to clean up a component, simply clear its check box.
- If required, you can dig deeper by expanding a component and selecting/unselecting its contents.

Having specified the components for clean-up, click the **Clean-up** button to continue.

Windows 7 and later operating systems do not store information on file and computer searches. Furthermore, information on opened/saved files is stored in the registry differently, so the wizard shows this information in a different way.

11.6.2.5 Clean-up progress

The operation status window reports about the state of the current operation.

The progress bar indicates the level of completion of the selected operation.

In some cases, the operation may take a long time to be completed. If this is the case, select the **Shutdown the computer after completion** check box. When the operation finishes, Acronis True Image will turn the computer off.

11.6.3 Hard Disk Wiping methods

What is the problem?

Information removed from a hard disk drive by non-secure means (for example, by simple Windows delete) can easily be recovered. Utilizing specialized equipment, it is possible to recover even repeatedly overwritten information.

Leakage mechanism

Data is stored on a hard disk as a binary sequence of 1 and 0 (ones and zeros), represented by differently magnetized parts of a disk.

Generally speaking, a 1 written to a hard disk is read as 1 by its controller, and 0 is read as 0. However, if you write 1 over 0, the result is conditionally 0.95 and vice versa – if 1 is written over 1 the result is 1.05. These differences are irrelevant for the controller. However, using special equipment, one can easily read the «underlying» sequence of 1's and 0's.

Copyright © Acronis International GmbH, 2002-2016

Information wiping methods used by Acronis

The detailed theory of guaranteed information wiping is described in an article by Peter Gutmann. Please see "Secure Deletion of Data from Magnetic and Solid-State Memory" at http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html.

No.	Algorithm (writing method)	Passes	Record
1.	United States Department of Defense 5220.22-M	4	1st pass – randomly selected symbols to each byte of each sector, 2 – complementary to written during the 1st pass; 3 – random symbols again; 4 – writing verification.
2.	United States: NAVSO P-5239-26 (RLL)	4	1st pass – 0x01 to all sectors, 2 – 0x27FFFFFF, 3 – random symbol sequences, 4 – verification.
3.	United States: NAVSO P-5239-26 (MFM)	4	1st pass – 0x01 to all sectors, 2 – 0x7FFFFFFF, 3 – random symbol sequences, 4 – verification.
4.	German: VSITR	7	1st – 6th – alternate sequences of: 0x00 and 0xFF; 7th – 0xAA; i.e. 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA.
5.	Russian: GOST P50739-95	1	Logical zeros (0x00 numbers) to each byte of each sector for 6th to 4th security level systems. Randomly selected symbols (numbers) to each byte of each sector for 3rd to 1st security level systems.
6.	Peter Gutmann's method	35	Peter Gutmann's method is very sophisticated. It's based on his theory of hard disk information wiping (see Secure Deletion of Data from Magnetic and Solid-State Memory).
7.	Bruce Schneier's method	7	Bruce Schneier offers a seven-pass overwriting method in his Applied Cryptography book. 1st pass – 0xFF, 2nd pass – 0x00, and then five times with a cryptographically secure pseudo-random sequence.
8.	Fast	1	Logical zeros (0x00 numbers) to all sectors to wipe.

11.7 Mounting an image

Mounting images as virtual drives lets you access them as though they were physical drives. Such ability means that:

- A new disk appears in your system.
- You can view the image contents in File Explorer and other file managers in read-only mode.

The operations described in this section are supported only for the FAT and NTFS file systems.

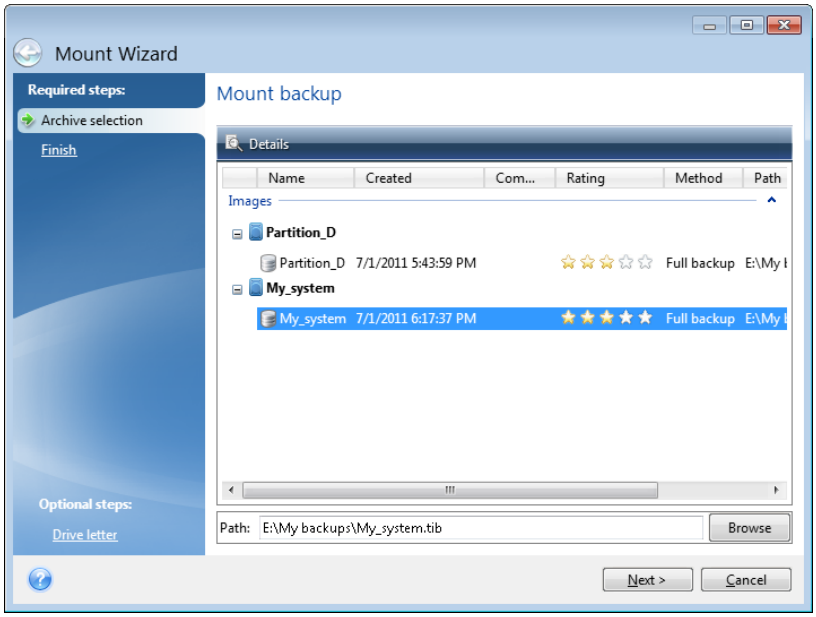
You cannot mount a disk backup, if it is stored on an FTP server.

How to mount an image

1. In File Explorer, right-click the image file that you want to mount, and then click **Mount image**.
   The Mount wizard opens.
2. Select the backup for mounting by its creation date/time. Thus, you can explore the data state at a certain moment.

Copyright © Acronis International GmbH, 2002-2016

Note that you cannot mount an image of the entire disk except in the case when the disk consists of one partition.



3. [optional step] On the **Drive letter** step, select a letter to be assigned to the virtual disk from the **Mount letter** drop-down list. If you do not want to mount a partition, select **Do not mount** in the list or clear the partition's check box.
4. Click **Proceed**.
5. After the image is connected, the program will run File Explorer, showing its contents.

11.8 Unmounting an image

We recommend that you unmount the virtual disk after all necessary operations are finished, as maintaining virtual disks takes considerable system resources.

To unmount an image, perform one of the following:

- In File Explorer, right-click the disk icon and click **Unmount**.
- Restart or shut down your computer.

11.9 Acronis Universal Restore

Acronis Universal Restore allows you to create a bootable system clone on different hardware. Use this utility when recovering your system disk to a computer with a dissimilar processor, different motherboard or a different mass storage device than in the system you originally backed up. This may be useful, for example, after replacing a failed motherboard or when deciding to migrate the system from one computer to another.

What problem does it solve?

A system disk image can be restored easily on the hardware where it was created or to identical hardware. However, if you try to do it on a dissimilar hardware, the recovered system will fail to

Copyright © Acronis International GmbH, 2002-2016

boot. This is because the new hardware is incompatible with critical drivers included in the image. The utility finds and installs drivers for devices that are critical for the operating system start-up, such as storage controllers, motherboard, or chipset.

How do I use it?

Before you start recovery to dissimilar hardware, ensure that you have:

- Backup of your system disk (p. 41) or Entire PC backup (p. 18)
- Acronis bootable media (p. 123)
- Acronis Universal Boot media (p. 158)

If you have Acronis True Image and Acronis Universal Boot Media Builder installed on your computer, you can place both Acronis True Image and Acronis Universal Boot on the same media. Refer to Creating Acronis Universal Boot media (p. 158) for details.

To recover your system to dissimilar hardware:

1. Start your target computer by using Acronis bootable media, and then recover your system from your system backup or Entire PC backup. Refer to Recovering your system to a new disk under bootable media (p. 73) for details.
2. Start your target computer by using Acronis Universal Boot media, and then follow the on-screen instructions to make your system bootable. Refer to Using Acronis Universal Restore (p. 160) for details.

11.9.1 Creating Acronis Universal Boot media

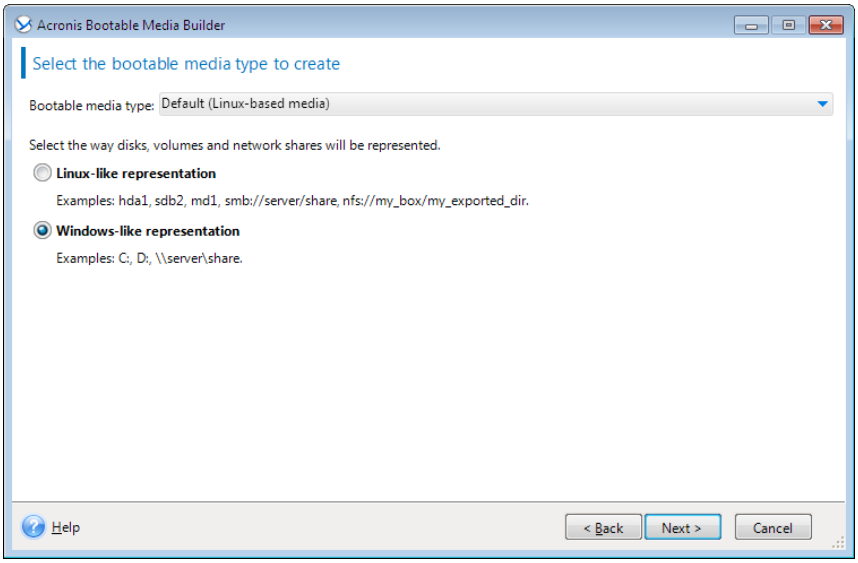
Acronis Universal Boot media is used to make your computer bootable after recovery to dissimilar hardware. Refer to Acronis Universal Restore (p. 157) for details.

To create Acronis Universal Boot media:

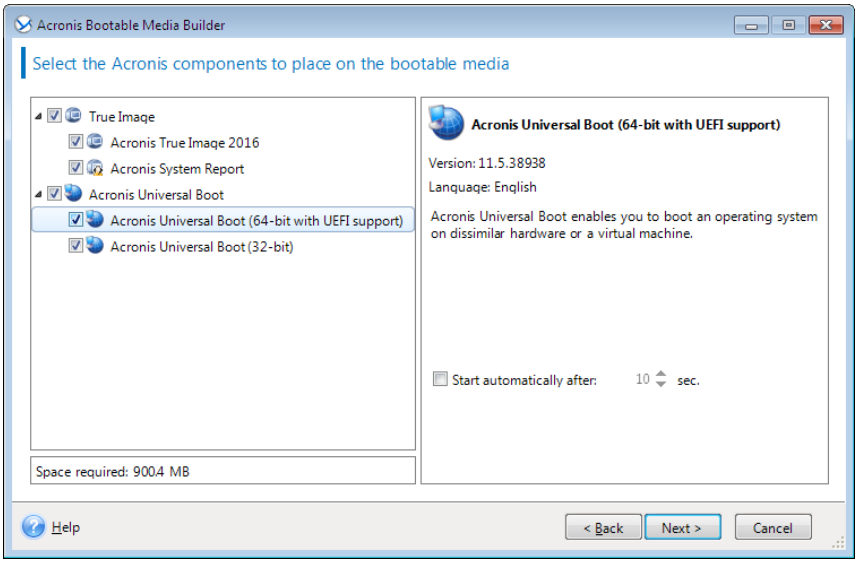
1. Start Acronis True Image.
2. In the **Tools** section, click **Acronis Universal Restore**.
3. Click **Download** to obtain Acronis Universal Boot Media Builder.
4. Run the downloaded file and install the media builder.
5. Plug in the USB flash drive or insert blank DVD that you want to make bootable.
6. To start Acronis Universal Boot Media Builder, perform one of the following:
   - In the **Tools** section, click **Acronis Universal Restore**.
   - Click the **Start** button, open the list of installed programs, and then click **Run Universal Boot Media Builder**.
7. Ensure that:
   - Linux-based media is selected as a bootable media type.

Copyright © Acronis International GmbH, 2002-2016

- Windows-like representation is selected as a way the disks and volumes are represented.


Acronis Bootable Media Builder
Select the bootable media type to create
Bootable media type: Default (Linux-based media)
Select the way disks, volumes and network shares will be represented.
Linux-like representation
Examples: hda1, sdb2, md1, smb://server/share, nfs://my_box/my_exported_dir.
Windows-like representation
Examples: C:, D:, \\server\share.
Help
< Back
Next >
Cancel

8. [Optional] Specify Linux kernel parameters. Refer to Bootable media startup parameters (p. 123) for details.
9. Select the Acronis components to place on the media.


Acronis Bootable Media Builder
Select the Acronis components to place on the bootable media
True Image
Acronis True Image 2016
Acronis System Report
Acronis Universal Boot
Acronis Universal Boot (64-bit with UEFI support)
Acronis Universal Boot (32-bit)
Acronis Universal Boot (64-bit with UEFI support)
Version: 11.5.38938
Language: English
Acronis Universal Boot enables you to boot an operating system on dissimilar hardware or a virtual machine.
Start automatically after: 10 sec.
Space required: 900.4 MB
Help
< Back
Next >
Cancel

You can select 32-bit and/or 64-bit components. The 32-bit components can work on 64-bit hardware. However, you need 64-bit components to boot a 64-bit computer that uses Unified Extensible Firmware Interface (UEFI).

To use the media on different types of hardware, select both types of components. When booting a machine from the resulting media, you will be able to select 32-bit or 64-bit components on the boot menu.

If Acronis True Image is installed on your computer, you can place it on the media as well. In this case, you will have a single bootable media containing both components required for recovery to dissimilar hardware.

10. Select a destination for the media:
    - **CD**
    - **DVD**
    - **USB flash drive**

Copyright © Acronis International GmbH, 2002-2016

- **ISO image file**

  You will need to specify the .iso file name and the destination folder.

  When the .iso file is created, you can burn it onto a CD or DVD. For example, in Windows 7 and later, you can do this using a built-in burning tool. In File Explorer, double-click the created ISO image file, and then click **Burn**.

11. Specify the mass storage drivers to be used by Acronis Universal Boot.

    You do not have to add the drivers now. You can do this later when you apply Acronis Universal Boot to a computer.

12. Click **Proceed**.

    When the media is created, unplug it from your computer. This is your Acronis Universal Boot media.

11.9.2 Using Acronis Universal Restore

Preparation

Prepare drivers

Before applying Universal Restore to a Windows operating system, make sure that you have the drivers for the new HDD controller and the chipset. These drivers are critical to start the operating system. Use the CD or DVD supplied by the hardware vendor or download the drivers from the vendor's website. The driver files should have the *.inf, *.sys or *.oem extensions. If you download the drivers in the *.exe, *.cab or *.zip format, extract them using a third-party application.

Check access to the drivers in bootable environment

Make sure you have access to the device with drivers when working under bootable media. Use WinPE-based media if the device is available in Windows but Linux-based media does not detect it.

Universal Restore settings

Automatic driver search

Specify where the program will search for the Hardware Abstraction Layer (HAL), HDD controller driver and network adapter driver(s):

- If the drivers are on a vendor's disc or other removable media, turn on the **Search removable media**.
- If the drivers are located in a networked folder or on the bootable media, specify the path to the folder by clicking **Add folder**.

In addition, Universal Restore will search the Windows default driver storage folder (usually WINDOWS/inf).

Mass storage drivers to install anyway

You need this setting if:

- The hardware has a specific mass storage controller such as RAID (especially NVIDIA RAID) or a fibre channel adapter.
- If the automatic drivers search does not help to boot the system.

Specify the appropriate drivers by clicking **Add driver**. The drivers defined here will be installed, with appropriate warnings, even if the program finds a better driver.

Copyright © Acronis International GmbH, 2002-2016

Universal Restore process

After you have specified the required settings, click **OK**.

When the process is complete, you will be able to configure the network connection and specify drivers for the video adapter, USB and other devices.

Copyright © Acronis International GmbH, 2002-2016

12 Troubleshooting

In this section

Acronis System Report 162
Acronis Smart Error Reporting 163
Sending feedback to Acronis 164
How to collect crash dumps 165
Acronis Customer Experience Program 165

12.1 Acronis System Report

When you contact the Acronis support team, they will usually need information about your system in order to resolve your problem. Sometimes getting the information is an inconvenient process and may take a long time. The Generate system report tool simplifies the procedure. It generates a system report containing all the necessary technical information and allows you to save the information to file. When it's necessary, you can attach the created file to your problem description and send it to Acronis support team. This will simplify and speed up the search for a solution.

To generate a system report, perform one of the following:

- On the sidebar, click **Help**, and then click **Generate system report**.
- On the Windows **Start** menu, click **All Programs** -> **Acronis** -> **Acronis True Image** -> **Tools and Utilities** -> **Acronis System Report**.
- Press **CTRL+F7**. Note that you can use the key combination even when Acronis True Image is performing any other operation.

After the report is generated:

- To save the generated system report to file, click **Save** and in the opened window specify a location for the created file.
- To exit to the main program window without saving the report, click **Cancel**.

You can place the tool on your bootable rescue media as a separate component to generate a system report when your computer cannot boot. After you boot from the media, you can generate the report without running Acronis True Image. Simply plug in a USB flash drive and click the **Acronis System Report** icon. The generated report will be saved on the USB flash drive.

To place the Acronis System Report tool on a bootable rescue media:

- Select the **Acronis System Report** check box on the **Rescue Media Content Selection** page of the **Acronis Media Builder** wizard.
- Click **Next** to continue.

Creating a system report from the command line prompt

1. Run Windows Command Processor (cmd.exe) as administrator.
2. Change the current directory to the Acronis True Image installation folder. To do so, enter:
   ```
   cd C:\Program Files (x86)\Acronis\TrueImageHome
   ```
3. To create the system report file, enter:
   ```
   SystemReport
   ```
   File SystemReport.zip will be created in the current folder.

Copyright © Acronis International GmbH, 2002-2016

If you want to create the report file with a custom name, type the new name instead of <file name>:

```
SystemReport.exe /filename:<file name>
```

To generate a system report under bootable media:

1. Create Acronis bootable rescue media, if you do not have it. See details in Acronis Media Builder (p. 122).
2. Arrange the boot order in BIOS so as to make your rescue media device (CD, DVD or USB stick) the first boot device. See Arranging boot order in BIOS (p. 81).
3. Boot from the rescue media and select **Acronis True Image**.

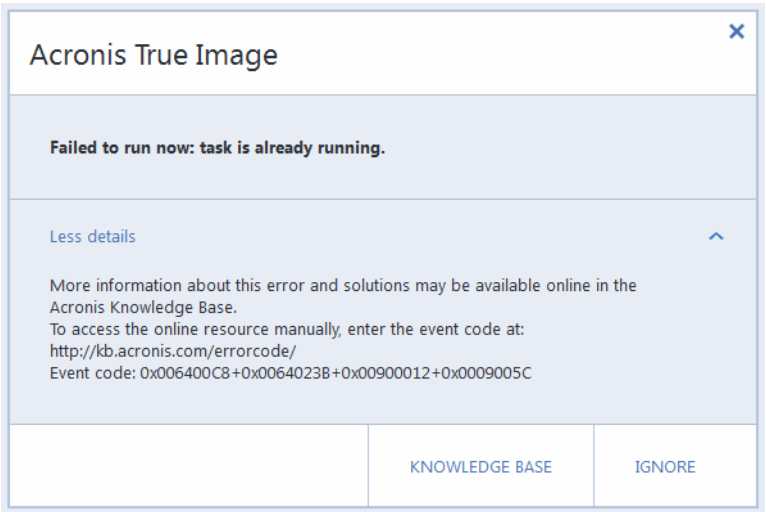
   *Instead of clicking **Acronis True Image**, you can plug in a USB flash drive and click **Acronis System Report**. In this case the program generates a report and automatically saves it to the flash drive.*

4. Click the arrow next to the Help icon ( ), and select **Generate system report**.
5. After the report is generated, click **Save** and in the opened window specify a location for the created file.

   The program will archive the report into a zip file.

12.2 Acronis Smart Error Reporting

When an issue is caused by an error in the program's operation, Acronis True Image displays an appropriate error message. The error message contains an event code and a short description of the error.


Acronis True Image
Failed to run now: task is already running.
Less details
More information about this error and solutions may be available online in the Acronis Knowledge Base.
To access the online resource manually, enter the event code at:
http://kb.acronis.com/errorcode/
Event code: 0x006400C8+0x0064023B+0x00900012+0x0009005C
KNOWLEDGE BASE
IGNORE

When you have an Internet connection

To view the Acronis Knowledge Base article suggesting a solution(s) for correcting the error, click the **Knowledge Base** button.

This will open a confirmation window that lists the information to be sent via Internet to the Acronis Knowledge Base. Click **OK** to permit sending the information.

If in future you would like to send such information without confirmation, select the **Always send without confirmation** check box.

Copyright © Acronis International GmbH, 2002-2016

When you do not have an Internet connection

1. In the error message window, please click **More details** and write down the event code. The code may look like this:

- 0x000101F6 - example of an ordinary event code.
- 0x00970007+0x00970016+0x00970002 - example of a composite event code. A code of this kind may appear when an error occurred in a low-level program module and then propagated to higher-level modules, resulting in errors in those modules as well.

1. When you establish Internet connection or if you can use another computer where Internet connection is available, enter the vent code at: http://kb.acronis.com/errorcode/.

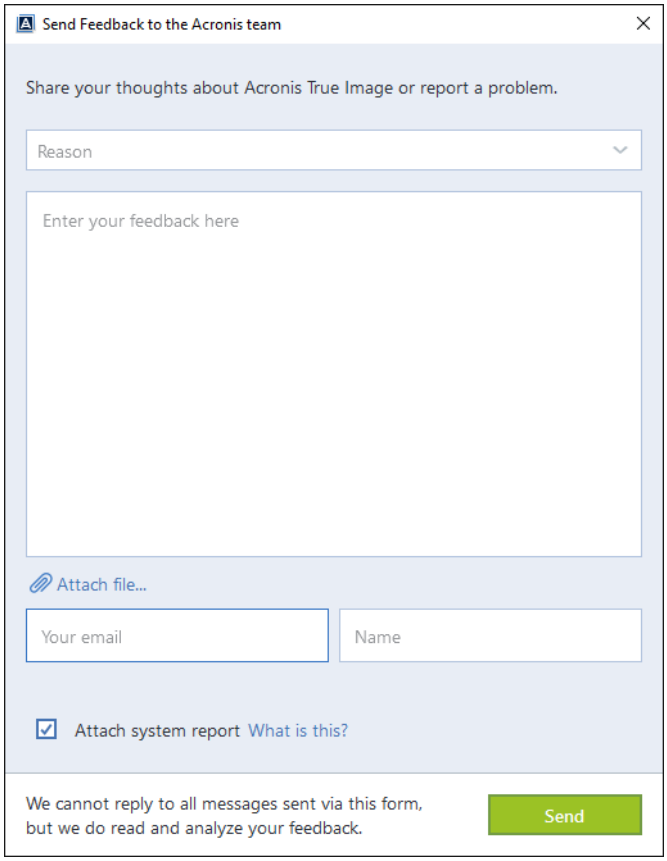
If the event code is not recognized in the Knowledge Base, the base does not yet contain an article to resolve the issue. In such cases, please open a trouble ticket with Acronis Customer Central.

12.3 Sending feedback to Acronis

We frequently improve our products and services by making them more functional, reliable, and fast. Via the feedback form, you can point out inconveniences and defects that we should resolve to make Acronis True Image even better. Please spend a couple of minutes to tell us what you think about our product, suggest a new feature, or report a problem. We do read and analyze all feedback.

To send a feedback to Acronis:

1. On the sidebar, click **Help**, and then click **Send feedback**. The feedback form opens.


Send Feedback to the Acronis team
Share your thoughts about Acronis True Image or report a problem.
Reason
Enter your feedback here
Attach file...
Your email
Name
Attach system report What is this?
We cannot reply to all messages sent via this form, but we do read and analyze your feedback.
Send

2. Choose a feedback reason from the list.
3. Type your message.
4. Provide your name and email.

Copyright © Acronis International GmbH, 2002-2016

5. [Optional step] You can also attach a file and Acronis system report. Refer to Acronis System Report (p. 162) for details.

   We recommend that you attach the system report when you faced a serious error, for example, when Acronis True Image stopped responding.
6. Click **Send**.

12.4 How to collect crash dumps

Because a crash of Acronis True Image or Windows can be caused by different reasons, each crash case must be investigated separately. Acronis Customer Central would appreciate if you could provide the following information:

If Acronis True Image crashes, please provide the following information:

1. A description of the exact sequence of steps performed before you encountered the issue.
2. A crash dump. For information on how to collect such a dump, see the Acronis Support Knowledge Base (KB) article at http://kb.acronis.com/content/27931.

If Acronis True Image causes a Windows crash:

1. A description of the exact sequence of steps performed before you encountered the issue.
2. A Windows dump file. For information on how to collect such a dump see the Acronis Support KB article at http://kb.acronis.com/content/17639.

If Acronis True Image hangs:

1. A description of the exact sequence of steps performed before you encountered the issue.
2. A userdump of the process. See the Acronis Support KB article at http://kb.acronis.com/content/6265.
3. The Procmon log. See the Acronis Support KB article at http://kb.acronis.com/content/2295.

If you cannot access the information, contact Acronis Customer Central for an FTP link for uploading files.

This information will speed up the process of finding a solution.

12.5 Acronis Customer Experience Program

Acronis Customer Experience Program (CEP) is a new way to allow Acronis customers to contribute to the features, design and development of Acronis products. This program enables our customers to provide us with various information, including information about the hardware configuration of your host computer and/or virtual machines, the features you use most (and least), and the nature of the problems you face. Based on this information, we will be able to improve the Acronis products and the features you use most often.

To make a decision:

1. On the sidebar, click **Settings**.
2. To leave the program, clear the **Participate in the Acronis Customer Experience Program** check box.

If you choose to participate, the technical information will be automatically collected every 90 days. We will not collect any personal data, like your name, address, phone number, or keyboard input. Participation in the CEP is voluntary, but the end results intended to provide software improvements and enhanced functionality to better meet the needs of our customers.

Copyright © Acronis International GmbH, 2002-2016

Copyright Statement

Copyright © Acronis International GmbH, 2002-2016. All rights reserved.

"Acronis", "Acronis Compute with Confidence", "Acronis Recovery Manager", "Acronis Secure Zone", Acronis True Image, Acronis Try&Decide, and the Acronis logo are trademarks of Acronis International GmbH.

Linux is a registered trademark of Linus Torvalds.

VMware and VMware Ready are trademarks and/or registered trademarks of VMware, Inc. in the United States and/or other jurisdictions.

Windows and MS-DOS are registered trademarks of Microsoft Corporation.

All other trademarks and copyrights referred to are the property of their respective owners.

Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of this work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

DOCUMENTATION IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Third party code may be provided with the Software and/or Service. The license terms for such third-parties are detailed in the license.txt file located in the root installation directory. You can always find the latest up-to-date list of the third party code and the associated license terms used with the Software and/or Service at http://kb.acronis.com/content/7696

Acronis patented technologies

Technologies, used in this product, are covered and protected by one or more U.S. Patent Numbers: 7,047,380; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121 and patent pending applications.

13 Glossary of Terms

A

Acronis Secure Zone

A secure partition for storing backups (p. 167) on a hard disk. Advantages:

- enables recovery of a disk to the same disk where the disk's backup resides
- offers a cost-effective and handy method for protecting data from software malfunction, virus attack, operator error
- eliminates the need for a separate media or network connection to back up or recover the data

Limitations:

1) The Acronis Secure Zone cannot be created on a dynamic disk.

2) The Acronis Secure Zone is not available as a location for backups in the recovery environment when you start Acronis True Image from bootable rescue media, through Acronis Startup Recovery Manager or BartPE.

Acronis Startup Recovery Manager

A protection tool that allows to start standalone version of Acronis True Image at boot time when F11 is pressed. Acronis Startup Recovery Manager eliminates the need for rescue media.

Acronis Startup Recovery Manager is especially useful for mobile users. If a failure occurs, the user reboots the machine, hits F11 on prompt "Press F11 for Acronis Startup Recovery Manager..." and performs data recovery in the same way as with ordinary bootable media.

Limitations: cannot be organized on a dynamic disk; requires manual configuration of boot loaders, such as LILO and GRUB; requires re-activation of third-party loaders.

B

Backup

1. The same as Backup operation (p. 167).
2. A set of backup versions created and managed by using backup settings. A backup can contain multiple backup versions created using full (p. 168) and incremental (p. 168) backup methods. Backup versions belonging to the same backup are usually stored in the same location.

Backup operation

An operation that creates a copy of the data that exists on a machine's hard disk for the purpose of recovering or reverting the data to a specified date and time.

Backup settings

A set of rules configured by a user when creating a new backup. The rules control the backup process. Later you can edit the backup settings to change or optimize the backup process.

Backup version

The result of a single backup operation (p. 167). Physically, it is a file or a set of files that contains a copy of the backed up data as of a specific date and time. Backup version files created by Acronis True Image have a TIB extension. The TIB files resulting from consolidation of backup versions are also called backup versions.

Backup version chain

Sequence of minimum 2 backup versions (p. 167) that consist of the first full backup version and the subsequent one or more incremental or differential backup versions. Backup version chain continues till the next full backup version (if any).

Bootable media

A physical media (CD, DVD, USB flash drive or other media supported by a machine BIOS as a boot device) that contains standalone version of Acronis True Image.

Bootable media is most often used to:

- recover an operating system that cannot start
- access and back up the data that has survived in a corrupted system
- deploy an operating system on bare metal
- create basic or dynamic volumes on bare metal
- back up sector-by-sector a disk that has an unsupported file system

D

Data synchronization

Data synchronization is a process of keeping data identical in two or more synchronized folders. These folders may be located on the same computer or on different computers connected via a local network or via the Internet. When you create, copy, modify or delete a file or a subfolder in your sync folder, the same action is automatically done in the other sync folders. And vice versa - when something changes in the other sync folders, the same change is done in your folder.

Differential backup

1. A backup method used for saving data changes that occurred since the last full backup version (p. 168) within a backup.
2. A backup process that creates a differential backup version (p. 168).

Differential backup version

A differential backup version stores changes to the data against the latest full backup version (p. 168). You need access to the corresponding full backup version to recover the data from a differential backup version.

Disk backup (Image)

A backup (p. 167) that contains a sector-based copy of a disk or a partition in packaged form. Normally, only sectors that contain data are copied. Acronis True Image provides an option to take a raw image, that is, copy all the disk sectors, which enables imaging of unsupported file systems.

F

Full backup

1. A backup method that is used to save all the data selected to back up.
2. A backup process that creates a full backup version (p. 168).

Full backup version

A self-sufficient backup version (p. 167) containing all data chosen for backup. You do not need access to any other backup version to recover the data from a full backup version.

I

Image

The same as Disk backup (p. 168).

Incremental backup

1. A backup method used for saving data changes that occurred since the last backup version (p. 167) (of any type) within a backup.
2. A backup process that creates an incremental backup version (p. 168).

Incremental backup version

A backup version (p. 167) that stores changes to the data against the latest backup version. You need access to other backup versions from the same backup (p. 167) to restore data from an incremental backup version.

Copyright © Acronis International GmbH, 2002-2016

N

Nonstop backup

Nonstop backup actually is a disk/partition or file backup that is created using the Acronis Nonstop Backup feature. This is a set of one full backup version (p. 168) and a sequence of incremental backup versions (p. 168) that are created at short intervals. It gives almost continuous protection of data, that is, it allows recovery of previous data state at any recovery point you need.

Nonstop protection

Nonstop protection - the process that the Nonstop Backup feature performs when it is turned on.

O

Online backup

Online backup - a backup that is created using Acronis Online Backup. Online backups are stored in a special storage named Acronis Cloud, accessible over the Internet. The main advantage of an online backup is that all backups are stored on the remote location. It gives a guarantee that all backed up data will be safe independently of a user local storages. To begin to use Acronis Cloud a user should subscribe to the service.

R

Recovery

Recovery is a process of returning of a corrupted data to a previous normal state from a backup (p. 167).

S

Sync

1. The same as Data synchronization (p. 168).
2. Sync settings which were configured on the sync owner's computer. A created sync is managed using the corresponding sync box. Sync creation does not mean start of sync process. Other users may join a created sync.

V

Validation

An operation that checks whether you will be able to recover data from a particular backup version (p. 167).

When you select for validation…

- a full backup version (p. 168) - the program validates the full backup version only.
- a differential backup version (p. 168) - the program validates the initial full backup version and the selected differential backup version.
- an incremental backup version (p. 168) - the program validates the initial full backup version, the selected incremental backup version, and the whole chain (if any) of backup versions to the selected incremental backup version. If the chain contains one or more differential backup versions, the program validates (in addition to the initial full backup version and the selected incremental backup version) only the most recent differential backup version in the chain and all subsequent incremental backup versions (if any) between the differential backup version and the selected incremental backup version.

Version of synced file

A state of a file which is located in a sync folder after each modification of this file. File versions may be stored on Acronis Cloud.

Copyright © Acronis International GmbH, 2002-2016